NETGEAR

N300 Wireless Router WNR2000v4

User Manual

350 East Plumeria Drive
San Jose, CA 95134
USA

February 2013
202-11229-01
v1.0

Support

Thank you for choosing NETGEAR.

After installing your device, locate the serial number on the label of your product and use it to register your product at *https://my.netgear.com*. You must register your product before you can use NETGEAR telephone support. NETGEAR recommends registering your product through the NETGEAR web site. For product updates and web support, visit *http://support.netgear.com*.

Phone (US & Canada only): 1-888-NETGEAR.

Phone (Other Countries): Check the list of phone numbers at *http://support.netgear.com/general/contact/default.aspx.*

NETGEAR recommends that you use only the official NETGEAR support resources.

Trademarks

NETGEAR, the NETGEAR logo, and Connect with Innovation are trademarks and/or registered trademarks of NETGEAR, Inc. and/or its subsidiaries in the United States and/or other countries. Information is subject to change without notice. © NETGEAR, Inc. All rights reserved.

Revision History

Publication Part Number	Version	Publish Date	Comments
202-11229-01	v1.0	February 2013	First publication

Contents

Chapter 1 Hardware Setup

Unpack Your Router 8
Hardware Features 8
Front Panel 9
Back Panel 10
Label 11
Position Your Router 11
Cable Your Router 13
Verify the Cabling 14

Chapter 2 Getting Started with NETGEAR genie

Router Setup Preparation 16
Use Standard TCP/IP Properties for DHCP 16
Gather ISP Information 16
Wireless Devices and Security Settings 16
Types of Logins and Access 16
NETGEAR genie Setup 17
Use NETGEAR genie after Installation 17
Upgrade Router Firmware 18
Router Dashboard (Basic Home Screen) 19
Change the Password 20
Password Recovery 21
Add Wireless Devices or Computers to Your Network 21
Manual Method 21
Wi-Fi Protected Setup (WPS) Method 22

Chapter 3 genie Basic Settings

Internet Setup 24
Internet Setup Screen Fields 25
Basic Wireless Settings 26
Wireless Settings Screen Fields 28
WPA-PSK, WPA2-PSK, and WPA-PSK + WPA2-PSK Mixed Mode . . . 29
WPA/WPA2 Enterprise 30
WEP 31
Attached Devices 32
Parental Controls 33
Guest Network 36

Chapter 4 genie Advanced Home

Setup Wizard 40
WPS Wizard 41
Setup Menu 42
WAN Setup 43
WAN Setup Screen Settings 43
Default DMZ Server 44
Change the MTU Size 45
LAN Setup 46
LAN Setup Screen Settings 47
Manage the DHCP Server on the Router 48
Set Up Address Reservation 49
QoS Setup 51
Wi-Fi Multimedia Quality of Service for Wireless Traffic 51
Quality of Service Priority Rules and Internet Access 51
Bandwidth Control 58

Chapter 5 Security

Keyword Blocking of HTTP Traffic 61
Exempt a Computer from Blocking and Logging 62
Block Services (Port Filtering) 62
Schedule Blocking 65
Security Event Email Notifications 66

Chapter 6 Administration

Upgrade the Router Firmware 69
View and Configure Logs 70
Manage the Configuration File 71
Back Up Settings 71
Restore Configuration Settings 72
Erase 72

Chapter 7 Advanced Settings

Advanced Wireless Settings 75
Advanced Settings for Your Wireless Network 75
Set Up a Wireless Schedule 76
Set Up the WPS Settings 77
Set Up a Wireless Card Access List 78
Wireless Access Point (AP) 80
Wireless Distribution System (WDS) 82
Set Up the Base Station 83
Set Up a Repeater 84
Port Forwarding and Port Triggering Configuration Concepts 86
Remote Computer Access Basics 86
Port Triggering to Open Incoming Ports 87

Port Forwarding to Permit External Host Communications 88
How Port Forwarding Differs from Port Triggering 89
Set Up Port Forwarding to Local Servers 90
Add a Custom Service 91
Edit or Delete a Port Forwarding Entry 92
Application Example: Make a Local Web Server Public 92
Set Up Port Triggering 93
Dynamic DNS 96
Static Routes 98
Remote Management 100
Universal Plug and Play 101
IPv6 103
Requirements for Entering IPv6 Addresses 104
IPv6 Auto Detect 104
IPv6 Auto Config 105
IPv6 6to4 Tunnel 107
IPv6 Pass Through 108
IPv6 Fixed 108
IPv6 DHCP 110
IPv6 PPPoE 111
Traffic Meter 112

Chapter 8 Monitoring

Router Status and Usage Information Screen 116
Router Information Pane 117
Internet Port Pane 117
Statistics 118
Connection Status 119
Wireless Settings Pane 120
Guest Network Pane 121

Chapter 9 Troubleshooting

Quick Tips 123
Sequence to Restart Your Network 123
Check Ethernet Cable Connections 123
Wireless Settings 123
Network Settings 123
Troubleshoot with the LEDs 124
Power LED Is Off or Blinking 124
Power LED Stays Amber 124
All LEDs Remain Lit after Startup 124
Internet or LAN Port LEDs Are Off 125
Wireless LED Is Off 125
The WPS (Push 'N' Connect) Button Blinks Amber 125
Cannot Log In to the Router 126
Cannot Access the Internet 126
Troubleshoot Internet Browsing 127

Troubleshoot a PPPoE Internet Connection. 128
Changes Not Saved 128
Wireless Connectivity 129
Wireless Signal Strength 129
Troubleshoot Your Network Using the Ping Utility 129
Test the LAN Path to Your Router 129
Test the Path from Your Computer to a Remote Device 130

Appendix A Supplemental Information

Factory Settings 133
Technical Specifications 134

Appendix B Notification of Compliance

Index

Hardware Setup

1

Get to know your router

If you have not already set up your new router using the installation guide that comes in the box, this chapter walks you through the hardware setup. *Chapter 2, Getting Started with NETGEAR genie*, explains how to set up your Internet connection.

This chapter contains the following sections:

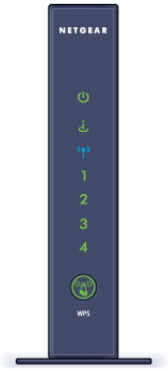
- *Unpack Your Router*
- *Hardware Features*
- *Position Your Router*
- *Cable Your Router*
- *Verify the Cabling*

For more information about the topics covered in this manual, visit the support website at *http://support.netgear.com*.

Firmware updates with new features and bug fixes are made available from time to time on *downloadcenter.netgear.com*. Some products can regularly check the site and download new firmware, or you can check for and download new firmware manually. If the features or behavior of your product does not match what is described in this guide, you might need to update your firmware.

Unpack Your Router

Open the box and remove the router, cables, and installation guide.



N300 Wireless Router

Ethernet cable

Power adapter

Figure 1. Package contents

Your box contains the following items:

- N300 Wireless Router WNR2000v4
- AC power adapter (plug varies by region)
- Category 5e (Cat 5E) Ethernet cable
- Installation guide

If any parts are incorrect, missing, or damaged, contact your NETGEAR dealer. Keep the carton and original packing materials, in case you need to return the product for repair.

Hardware Features

Before you cable your router, take a moment to become familiar with the label and the front and back panels. Pay particular attention to the LEDs on the front panel.

Front Panel

The router front panel has the following status LEDs and button:

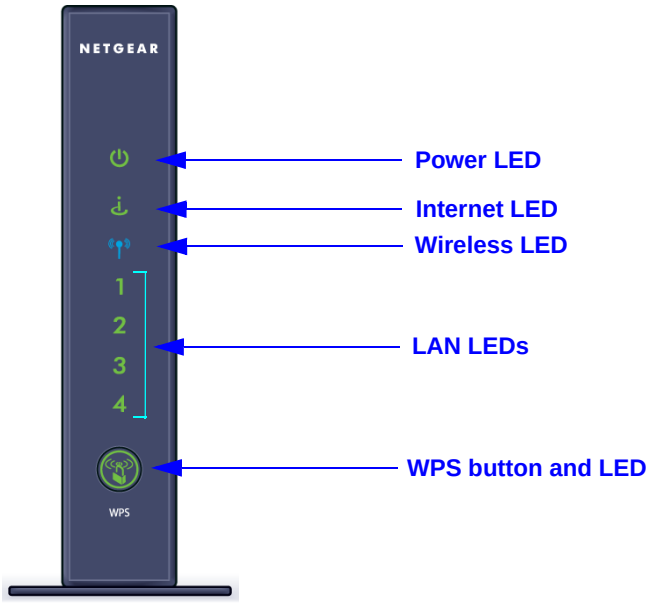


Figure 2. Front panel

Table 1. Front panel LED descriptions

LED	Description
Power	• **Solid amber**. The unit is starting up after being powered on. • **Solid green**. The power is on, and the router is ready. • **Blinking amber**. A firmware update is in progress. • **Blinking green**. The firmware is corrupt. • **Off**. Power is not supplied to the router.
Internet	• **Solid amber**. The IP address has not been acquired. • **Solid green**. An IP address has been received; ready to transmit data. • **Off**. No Ethernet cable is connected between the router and the modem.
Wireless	• **Solid blue**. The wireless radio is operating. • **Off**. The wireless radio is off.
LAN ports 1–4	• **Solid green**. The LAN port has detected a 100 Mbps link with an attached device. • **Solid amber**. The LAN port has detected a 10 Mbps link with an attached device. • **Off**. No link is detected on the LAN port.

Table 1. Front panel LED descriptions (continued)

LED	Description
WPS	• **Solid green**. Indicates that wireless security is enabled. • **Blinking green**. The router is attempting to use WPS to add a wireless device or computer to the wireless network. • **Blinking green rapidly for about 5 seconds**. WPS has failed to add a wireless device or computer. • **Blinking green rapidly and continuously**. The router is in stuck in the temporary AP setup locked state. For more information, see *The WPS (Push 'N' Connect) Button Blinks Amber* on page 125. • **Off**. No WPS connection exists.

Back Panel

The back panel has the following buttons, ports, and connector:

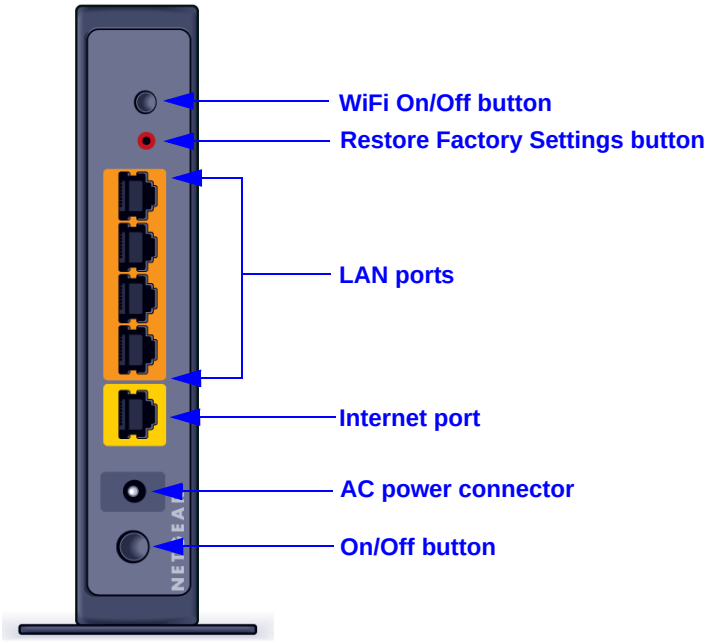


Figure 3. Back panel

Table 2. Back panel button, port, and connector descriptions

Port or Button	Description
WiFi On/Off button	Turns the wireless radio in the router on or off.
Restore Factory Settings button	Press and hold this button for about 7 seconds to reset the router to its factory default settings.
LAN ports	Four local area network (LAN) 10/100 Mbps Ethernet ports for connecting the router to your local computers.

Table 2. Back panel button, port, and connector descriptions (continued)

Port or Button	Description
Internet port	Ethernet port for connecting the router to a cable broadband modem or DSL broadband modem. The Internet port is also referred to as the WAN port.
AC power connector	AC power connector to connect the power adapter to the router.
Power On/Off button	Turns the router on or off.

Label

The label on the back panel of the router shows the default login information, default WiFi network name (SSID), network key (also referred to as wireless network password or passphrase), serial number, MAC address, and other information.

Figure 4. Label on the back panel

For information about restoring factory settings, see *Factory Settings* on page 133.

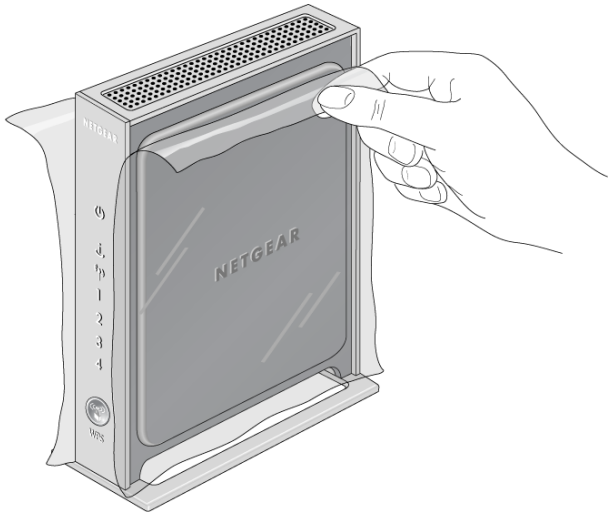
Position Your Router

The router lets you access your network from virtually anywhere within the operating range of your wireless network. However, the operating distance or range of your wireless connection can vary significantly depending on the physical placement of your router. For example, the thickness and number of walls the wireless signal passes through can limit the range. For best results, place your router:

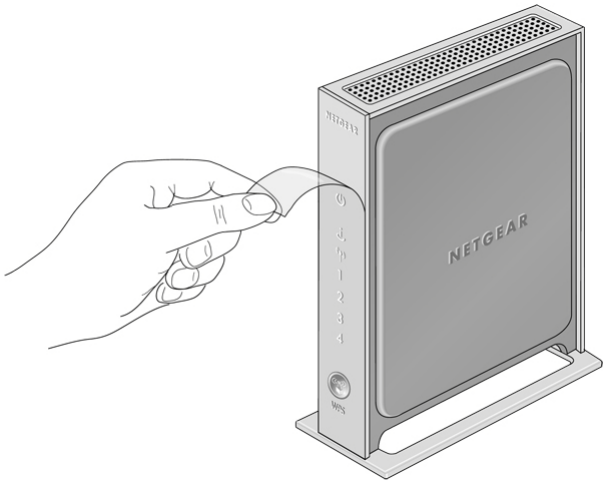
- Near the center of the area where your computers and other devices operate, and preferably within line of sight to your wireless devices.
- So it is accessible to an AC power outlet and near Ethernet cables for wired computers.
- In an elevated location such as a high shelf, keeping the number of walls and ceilings between the router and your other devices to a minimum.
- Away from electrical devices that are potential sources of interference, such as ceiling fans, home security systems, microwaves, computers, or the base of a cordless phone or 2.4 GHz cordless phone.
- Away from any large metal surfaces, such as a solid metal door or aluminum studs. Large expanses of other materials such as glass, insulated walls, fish tanks, mirrors, brick, and concrete can also affect your wireless signal.

➢ **To prepare your router for installation:**

1. Carefully peel off the protective film covering both sides of your router.



2. Remove the protective film covering the front panel of the router.

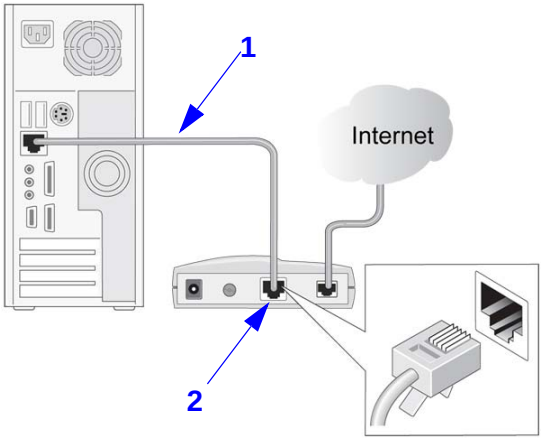


3. Place your router in a suitable area for installation (near an AC power outlet and accessible to the Ethernet cables for your wired computers).

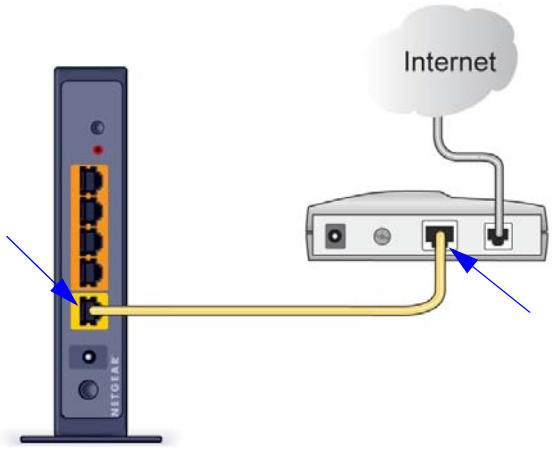
Cable Your Router

The installation guide that came in the box has a cabling diagram on the first page. This section describes how to connect the router, the computer, and the cable or DSL broadband modem, and provides detailed illustrations.

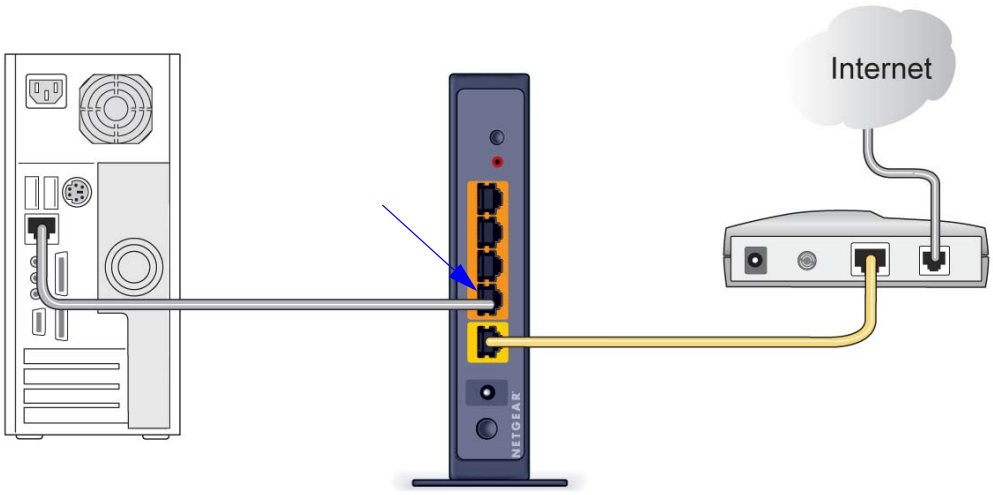
1. Turn off and unplug the cable or DSL broadband modem. If your modem has a backup battery, remove it as well.
2. Locate the Ethernet cable (1) that connects your computer to the modem.



3. Disconnect the cable from the modem (2). You will connect it to the router later.
4. Locate the Ethernet cable that came with the NETGEAR product. Securely insert the Ethernet cable into your modem and into the Internet port of the router.



5. Locate the cable you removed from the modem in *Step 3*. Securely insert that cable into a LAN port on the router such as LAN port 4.



Your network cables are connected, and you are ready to start your network. It is important that you start your network in the correct sequence:

1. First, power on the modem.
2. After the modem finishes starting up, power on the router. Turn on the router by pressing the **Power On/Off** button on the back.

Verify the Cabling

Verify that your router is cabled correctly by checking the router LEDs:

- The Power LED is solid green when the router is turned on.
- The Wireless LED is solid blue.
- The Internet LED is solid green. If it is not, make sure that the Ethernet cable is securely attached to the router Internet port, and that the modem is powered on.
- The LAN LEDs (1 through 4) are solid green or solid amber for any computers cabled to the router by an Ethernet cable.

Getting Started with NETGEAR genie

2

Connect to the router

This chapter explains how to use NETGEAR genie to set up your router after you complete cabling as described in the installation guide and in the previous chapter in this book.

This chapter contains the following sections:

- *Router Setup Preparation*
- *Types of Logins and Access*
- *NETGEAR genie Setup*
- *Use NETGEAR genie after Installation*
- *Upgrade Router Firmware*
- *Router Dashboard (Basic Home Screen)*
- *Change the Password*
- *Password Recovery*
- *Add Wireless Devices or Computers to Your Network*

Router Setup Preparation

You can set up your router with NETGEAR genie automatically, or you can use the genie menus and screens to set up your router manually. However, before you start the setup process, you need to have your ISP information on hand and make sure the laptops, computers, and other devices in the network have the settings described here.

Use Standard TCP/IP Properties for DHCP

If you set up your computer to use a static IP address, you need to change the settings so that it uses Dynamic Host Configuration Protocol (DHCP).

Gather ISP Information

If you have DSL broadband service, you might need the following information to set up your router and to check that your Internet configuration is correct. Your Internet service provider (ISP) should have provided you with all of the information needed to connect to the Internet. If you cannot locate this information, ask your ISP to provide it. When your Internet connection is working, you no longer need to launch the ISP's login program on your computer to access the Internet. When you start an Internet application, your router automatically logs you in.

- The ISP configuration information for your DSL account
- ISP login name and password
- Fixed or static IP address settings (special deployment by ISP; this is rare)

Wireless Devices and Security Settings

Make sure that the wireless device or computer that you are using supports WPA or WPA2 wireless security, which is the wireless security supported by the router. For information about the router's preconfigured security settings, see *Basic Wireless Settings* on page 26.

Types of Logins and Access

There are separate types of logins that have different purposes. It is important that you understand the difference so that you know which login to use when.

- **Router login** logs you in to the router user interface from NETGEAR genie. For more information, see *Use NETGEAR genie after Installation* on page 17.
- **ISP login** logs you in to your Internet service. Your service provider has provided you with this login information in a letter or some other way. If you cannot find this login information, contact your service provider.
- **Wireless network login**. Your router is preset with a unique wireless network name (SSID) and password for wireless access. This information is on the label located on the back of your router.

NETGEAR genie Setup

NETGEAR genie runs on any device with a web browser. It is the easiest way to set up the router because it automates many of the steps and verifies that those steps have been successfully completed. It takes about 15 minutes to complete.

➢ **To use NETGEAR genie to set up your router:**

1. Turn the router on by pressing the **Power On/Off** button, if not done yet.
2. Make sure that your device is connected with an Ethernet cable to your router.
3. Launch your Internet browser.
   - If this is the first time you are setting up the Internet connection for your router, the browser automatically goes to http://www.routerlogin.net, and the NETGEAR genie screen displays.
   - If you already used NETGEAR genie, type **http://www.routerlogin.net** in the address field for your browser to display the NETGEAR genie screen. For more information, see *Use NETGEAR genie after Installation* on page 17.
4. Follow the onscreen instructions to complete the NETGEAR genie setup.

   NETGEAR genie guides you through connecting the router to the Internet.

If the browser cannot display the web page:

- Make sure that the computer is connected to one of the four LAN Ethernet ports, or wirelessly to the router.
- Make sure that the router is fully up and running. Its Wireless LED should be lit.
- Close and reopen the browser to make sure that the browser does not cache the previous page.
- Browse to **http://routerlogin.net**.
- If the computer is set to a static or fixed IP address (this is uncommon), change it to obtain an IP address automatically from the router.

If the router does not connect to the Internet:

1. Review the router's settings to be sure that you have selected the correct options and typed everything correctly.
2. Contact your ISP to verify that you have the correct configuration information.
3. Read *Chapter 9, Troubleshooting*. If problems persist, register your NETGEAR product and contact NETGEAR technical support.

Use NETGEAR genie after Installation

When you first set up your router, NETGEAR genie automatically starts when you launch an Internet browser on a computer that is connected to the router.

➢ **To use NETGEAR genie again if you want to view or change settings for the router:**

1. Launch your browser from a computer or wireless device that is connected to the router.
2. Type **http://www.routerlogin.net** or **http://www.routerlogin.com**.

   The login window displays:

3. Enter **admin** for the router user name and **password** for the router password, both in lowercase letters.

   Note: *The router user name and password are different from the user name and password for logging in to your Internet connection. For more information, see Types of Logins and Access on page 16.*

Upgrade Router Firmware

When you set up your router and are connected to the Internet, the router automatically checks for you to see if newer firmware is available. If it is, a message is displayed on the top of the screen. The message might be *A router firmware upgrade is available*, or a similar message.

➢ **To upgrade the firmware after the router has detected newer firmware and displays a message:**

1. Click the message.

   The Firmware Upgrade Assistant displays.

2. Click **Yes**.

   The router upgrades to the latest firmware. After the upgrade, the router restarts.

CAUTION:

Do not try to go online, turn off the router, shut down the computer, or do anything else to the router until the router finishes restarting and the Power LED has stopped blinking and has turned to steady green for several seconds.

For more information about upgrading firmware, see *Upgrade the Router Firmware* on page 69.

Router Dashboard (Basic Home Screen)

The router Basic Home screen has a dashboard that lets you see the status of your Internet connection and network at a glance. You can click any of the five sections of the dashboard to view more detailed information. The left column has the menus, and at the top is an Advanced tab that provides access to additional menus and screens.

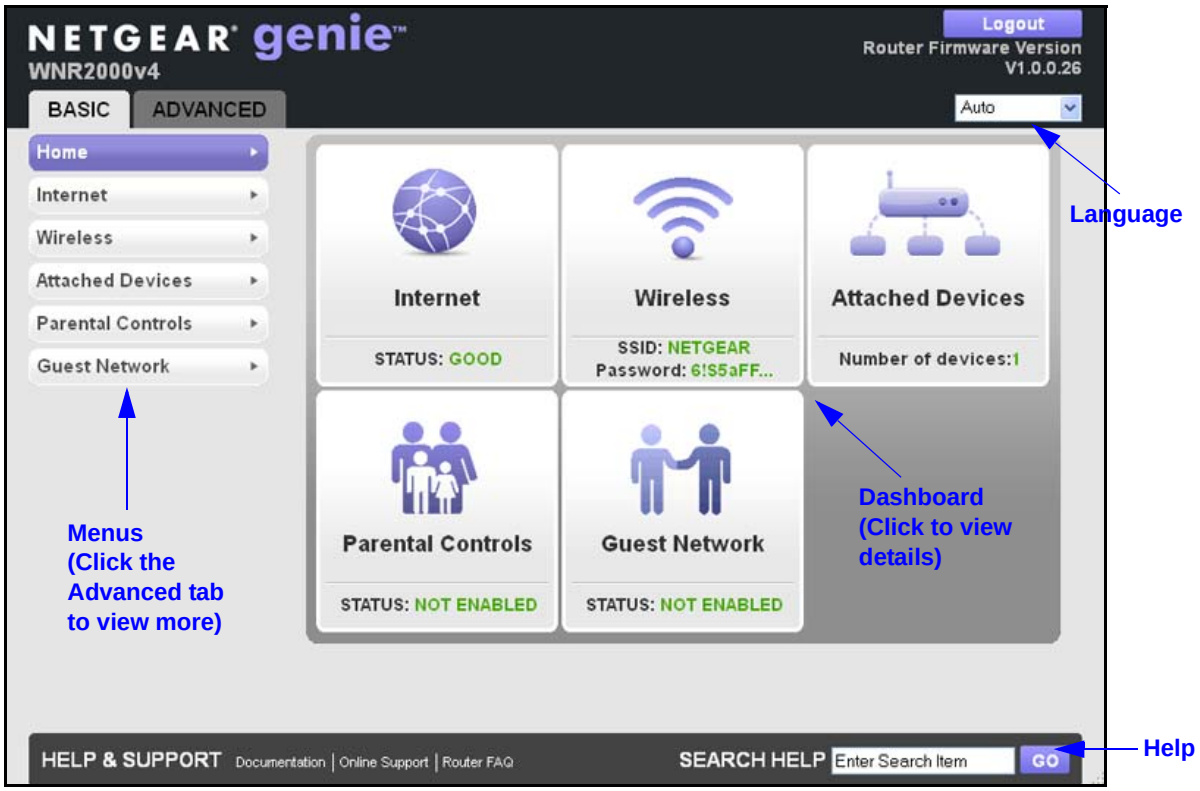


Figure 5. Router Basic Home screen with dashboard, language, and online help

Basic screen:

- **Home**. This dashboard screen displays when you log in to the router**.**
- **Internet**. Set, update, and check the ISP settings of your router.
- **Wireless**. View or change the wireless settings for your router.
- **Attached Devices**. View the devices that are connected to your network.
- **Parental Controls**. Download and set up parental controls to prevent objectionable content from reaching your computers.
- **Guest Network**. Set up a guest network to allow visitors to use your router's Internet connection.

Advanced tab. Set up the router for unique situations such as when remote access by IP address or by domain name from the Internet is needed. For more information, see *Chapter 7, Advanced Settings*. Using this tab requires a solid understanding of networking concepts.

Help & Support. Go to the NETGEAR support site to get information, help, and product documentation. These links work once you have an Internet connection.

Change the Password

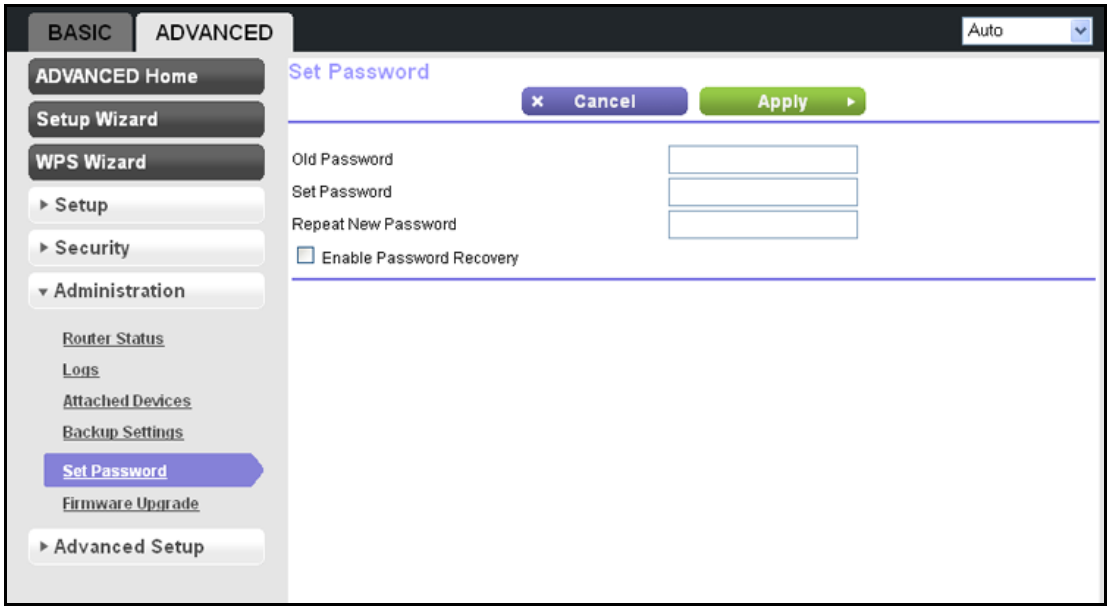
The default password that you use to log in to the router is admin. NETGEAR recommends that you change this default password to a secure password.

Changing the default password is not the same as changing the password for wireless access. The label on the back panel of your router shows your unique wireless network name (SSID) and the passphrase (also referred to as the wireless network password or network key) for wireless access (see *Label* on page 11).

➢ **To change the default password that you use to log in to the router:**

1. Select **Advanced > Administration > Set Password**.

   The Set Password screen displays:



2. Type the old password, and type the new password twice in the fields on this screen.
3. If you want to be able to recover the password, select the **Enable Password Recovery** check box.

   For more information, see the following section.

4. Click the **Apply** button.

Password Recovery

NETGEAR recommends that you enable password recovery if you change the password for the router's user name of admin. Then you have an easy way to recover the password if it is forgotten. This recovery process is supported in Internet Explorer, Firefox, and Chrome browsers, but not in the Safari browser.

➢ **To set up password recovery:**

1. Select **Advanced > Administration > Set Password**.

   The Set Password screen displays.

2. Select the **Enable Password Recovery** check box.
3. Select two security questions and provide answers to them.
4. Click the **Apply** button.

When you use your browser to access the router, the login window displays. If password recovery is enabled, when you click the Cancel button, the password recovery process starts. You can then enter the saved answers to the security questions to recover the password.

Add Wireless Devices or Computers to Your Network

Choose either the manual or the WPS method to add wireless devices and other equipment to your wireless network. For information about how to set up a guest network, see *Guest Network* on page 36.

Manual Method

➢ **To connect manually:**

1. Open the software that manages your wireless connections on the wireless device (laptop computer, gaming device, iPhone) that you want to connect to your router.

   This software scans for all wireless networks in your area.

2. Look for your network and select it. If you did not change the name of your network during the setup process, look for the default WiFi network name (SSID) and select it.

   The default SSID is located on the product label on the back panel of the router.

3. Enter the router wireless network password (passphrase) and click the **Connect** button.

   The default router passphrase is located on the product label on the back panel of the router.

4. Repeat steps 1–3 to add other wireless devices.

Wi-Fi Protected Setup (WPS) Method

Wi-Fi Protected Setup (WPS) lets you connect to a secure WiFi network without typing its password. Instead, press a button or enter a PIN. NETGEAR calls WPS Push 'N' Connect.

During the connection process, the client gets the security settings from the router so that every device in the network has the same security settings.

Some older WiFi equipment is not compatible with WPS. WPS works only with WPA2or WPA wireless security.

➢ **To use WPS to join the wireless network:**

1. Press the **WPS** button on the router front panel .

   The WPS LED (on the button) starts to blink green.

2. Within 2 minutes, press the **WPS** button on your wireless device, or follow the WPS instructions that came with the device.

   The device is now connected to your router.

3. Repeat steps 1–2 to add other WPS wireless devices.

genie Basic Settings

3

Your Internet connection and network

This chapter describes the features that are available from the genie Basic Home screen:

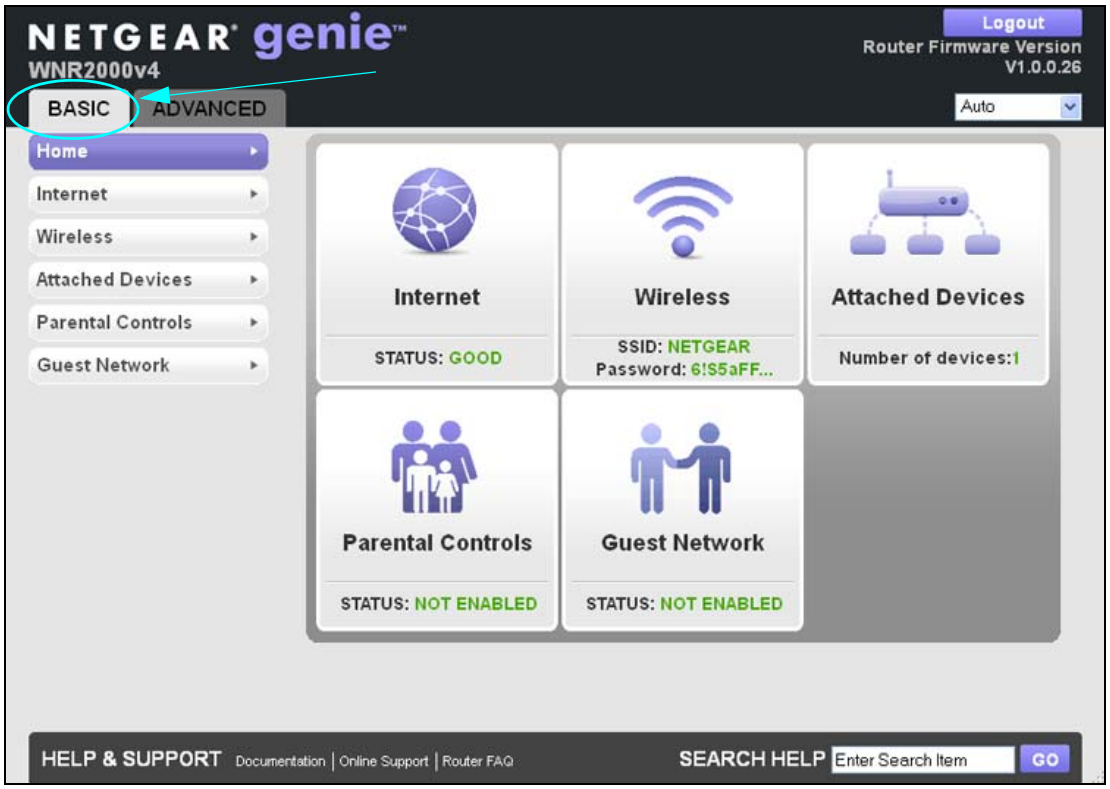


Figure 6. genie Basic Home screen

This chapter contains the following sections:

- *Internet Setup*
- *Basic Wireless Settings*
- *Attached Devices*
- *Parental Controls*
- *Guest Network*

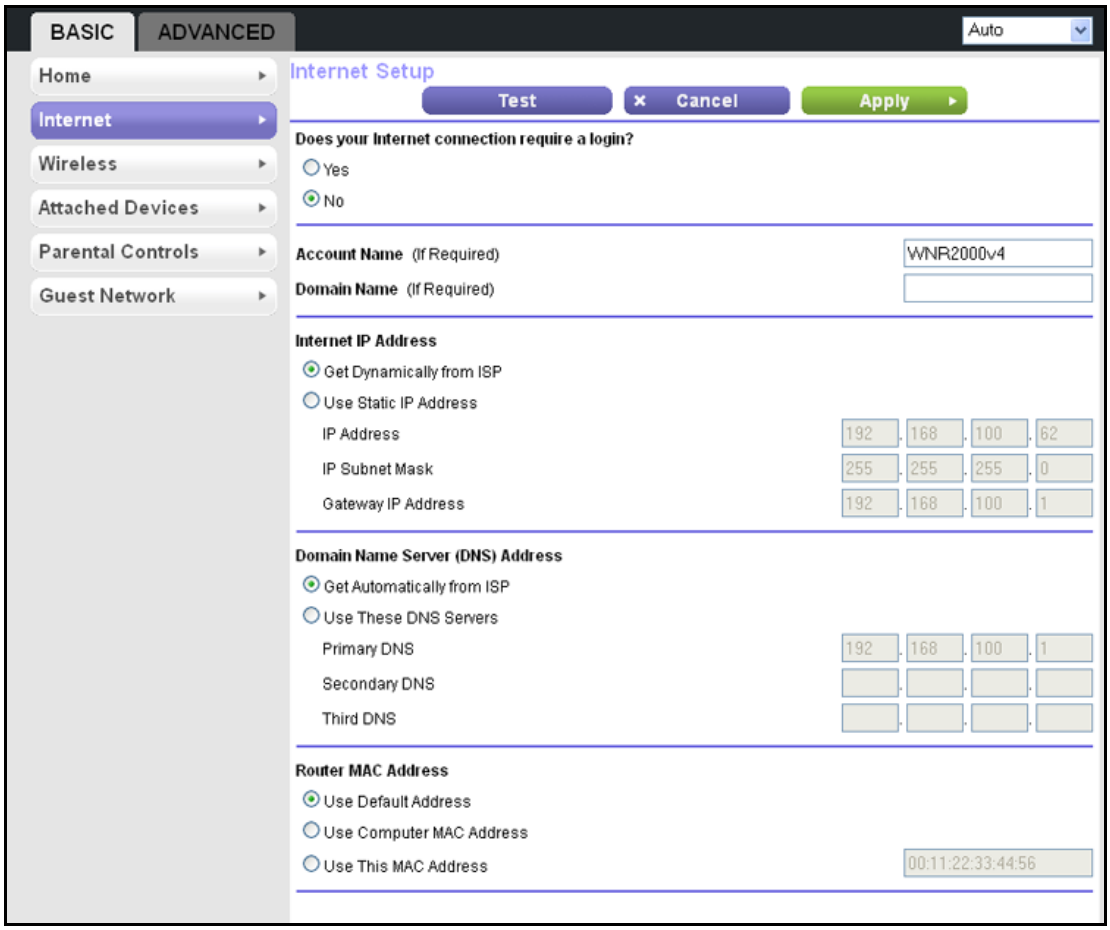
Internet Setup

The Internet Setup screen is where you view or change ISP information.

➢ **To view or change the Internet setup:**

1. From the Home screen, select **Internet**.

   The Internet Setup screen displays:



   The fields that display in the Internet Setup screen depend on whether your Internet connection requires a login.

   - **Yes**. Select the tunneling protocol, and enter the login name and password for your ISP. If you want to change the login time-out, enter a new value in minutes.
   - **No**. Enter the account and domain names, only if needed.

2. Enter the settings for the IP address and DNS server.

   The default settings usually work fine. If you have problems with your connection, check the ISP settings.

3. Click the **Apply** button.

4. Click the **Test** button.

   Your Internet connection is tested. If the router does not detect the Internet connection and the NETGEAR website does not display within 1 minute, see *Chapter 9, Troubleshooting*.

Internet Setup Screen Fields

The following descriptions explain all of the possible fields on the Internet Setup screen. Note that which fields display on this screen depends on whether an ISP login is required.

Does Your ISP Require a Login? Select either **Yes** or **No**.

These fields display when no login is required:

- **Account Name (If Required)**. Enter the account name provided by your ISP. This might also be called the host name.
- **Domain Name (If Required)**. Enter the domain name provided by your ISP.

These fields display when your ISP does require a login:

- **Internet Service Provider**. As the ISP tunneling protocol, select **PPTP**, **L2TP**, or **PPPoE**.
- **Login**. Enter the login name provided by your ISP. This is often an email address.
- **Password**. Enter the password that you use to log in to your ISP.
- **Service Name (If Required)**. Enter the service name provided by your ISP. If your ISP did not give you a service name, leave this field blank.
- **Connection Mode**. Select the one of the following connection modes:
  - **Always On**. The connection automatically starts when you turn on the router and does not time out. If the connection is terminated for some reason, the router attempts to bring up the connection.
  - **Dial on Demand**. The connection automatically starts when there is outbound traffic to the Internet and automatically terminates when the idle time-out period is exceeded.
  - **Manually Connect**. You need to connect and disconnect manually. To connect to the Internet, click the **Advanced** tab to display the Internet Port pane, click the **Connection Status** button to display the Connection Status screen (see *Connection Status* on page 119), and then click the **Connect** button. The manual connection does not time out. To disconnect from the Internet, click the **Disconnect** button. The Connect and Disconnect buttons display only when the connection mode is Manually Connect.
- **Idle Timeout (In Minutes)**. If you want to change the login time-out, enter a new value in minutes. This determines how long the router keeps the Internet connection active after there is no Internet activity from the LAN. Entering a value of 0 (zero) means never log out.

Internet IP Address.

- **Get Dynamically from ISP**. Your ISP uses DHCP to assign your IP address. Your ISP automatically assigns these addresses.
- **Use Static IP Address**. Enter the IP address, IP subnet mask, and the gateway IP address that your ISP assigned to you. The gateway is the ISP's router to which your router should connect.

Domain Name Server (DNS) Address. The DNS server is used to look up site addresses based on their names.

- **Get Automatically from ISP**. Your ISP uses DHCP to assign your DNS servers. Your ISP automatically assigns these IP addresses.
- **Use These DNS Servers**. If you know that your ISP does not automatically transmit DNS addresses to the router during login, select this option, and enter the IP address of your ISP's primary DNS server. If a secondary DNS server address is available, enter it also.

Router MAC Address. The Ethernet MAC address used by the router on the Internet port. Some ISPs register the MAC address of the network interface card in your computer when your account is first opened. They accept traffic only from the MAC address of that computer. This feature allows your router to use your computer's MAC address (this is also called spoofing or cloning).

- **Use Default Address**. Use the default MAC address.
- **Use Computer MAC Address**. The router captures and uses the MAC address of the computer that you are now using to configure the router. To configure the router, make sure that you use the computer that is registered and allowed by the ISP.
- **Use This MAC Address**. Enter the MAC address that you want to use.

Basic Wireless Settings

The Wireless Settings screen lets you view or configure the wireless network setup.

The router comes with preset WPA2-PSK security. This means that the WiFi network name (SSID), wireless network password (also referred to as the passphrase or network key), and security option (authentication and encryption protocol) are preset in the factory. You can find the preset SSID and password on the back panel of the router. The preset SSID and password are uniquely generated for every device to protect and maximize your wireless security.

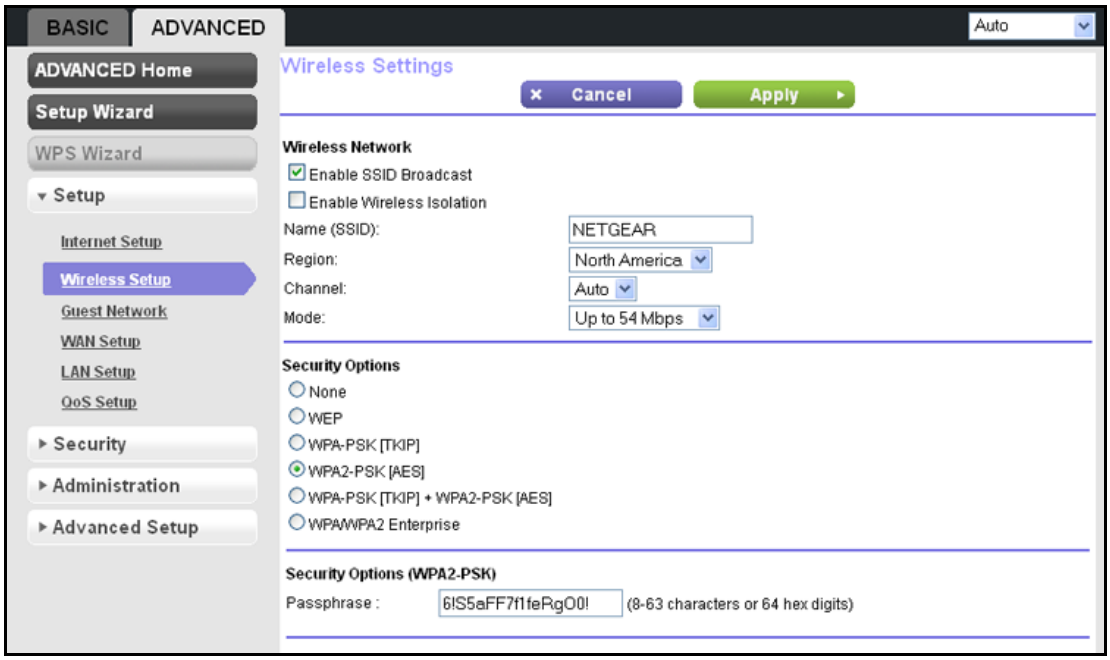
WARNING:

NETGEAR recommends that you do not change your preset security settings. If you do decide to change your preset security settings, make a note of the new settings and store it in a safe place where you can easily find it.

Note: If you use a wireless computer to change the wireless network name (SSID) or other wireless security settings, you are disconnected when you click the Apply button. To avoid this situation, use a computer with a wired connection to access the router.

➢ **To view or change basic wireless settings:**

1. On the Basic Home screen, select **Wireless** to display the Wireless Settings screen.



Note: *The screen sections, settings, and procedures are explained in the following sections.*

2. Make any changes that are needed.
3. Click the **Apply** button.
4. Set up and test your wireless devices and computers to make sure that they can connect wirelessly. If they do not, check the following:
   - Is your wireless device or computer connected to your network or another wireless network in your area? Some wireless devices automatically connect to the first open network (without wireless security) that they discover.
   - Does your wireless device or computer show up on the Attached Devices screen? If it does, then it is connected to the network.
   - If you are not sure what the network name (SSID) or password is, look on the label on the back panel of your router.

Note: The WEP option displays only if you select Up to 54 Mbps from the Mode menu.

Wireless Settings Screen Fields

The following sections describe the fields of the Wireless Settings screen.

Wireless Network

Enable SSID Broadcast. This setting allows the router to broadcast its SSID so wireless stations can see this wireless name (SSID) in their scanned network lists. This check box is selected by default, but you can clear it to disable broadcast of the SSID.

Enable Wireless Isolation. If this check box is selected, then wireless clients (computers or wireless devices) that join the network can use the Internet, but cannot access each other or access Ethernet devices on the network.

Name (SSID). The SSID is also known as the wireless network name. The default SSID is randomly generated. ***NETGEAR strongly recommends that you do not change the default SSID.*** If you do decide to change the name, enter a 32-character (maximum) name in this field. This field is case-sensitive.

Region. The location where the router is used. Select from the countries in the list. Note that in the United States, the region is fixed to United States and is not changeable.

Channel. This setting is the wireless channel used by the gateway. Enter a value from 1 through 13. (For products in the North America market, only Channels 1 through 11 can be operated.) Do not change the channel unless you experience interference (shown by lost connections or slow data transfers). If this happens, experiment with different channels to see which is the best. The default setting is Auto, which means that the router selects a channel automatically.

Note: *When you use multiple access points, it is better if adjacent access points use different channels to reduce interference. The recommended channel spacing between adjacent access points is 5 channels (for example, use Channels 1 and 6, or 6 and 11).*

Mode. Up to 150 Mbps is the default setting. Up to 54 Mbps supports 802.11g, and 11b wireless devices. The 300 Mbps setting allows 802.11n devices to connect at this speed.

Security Options

The Security Options section of the Wireless Settings screen lets you change the wireless authentication and encryption option and the passphrase (also referred to as the wireless network password or network key). The security that you select encrypts data transmissions and ensures that only trusted devices receive authorization to connect to your network.

WARNING:

NETGEAR recommends that you do not change the wireless security option and the passphrase. However, if you need to change these settings, the following sections explains how. Do not disable wireless security!

WPA-PSK, WPA2-PSK, and WPA-PSK + WPA2-PSK Mixed Mode

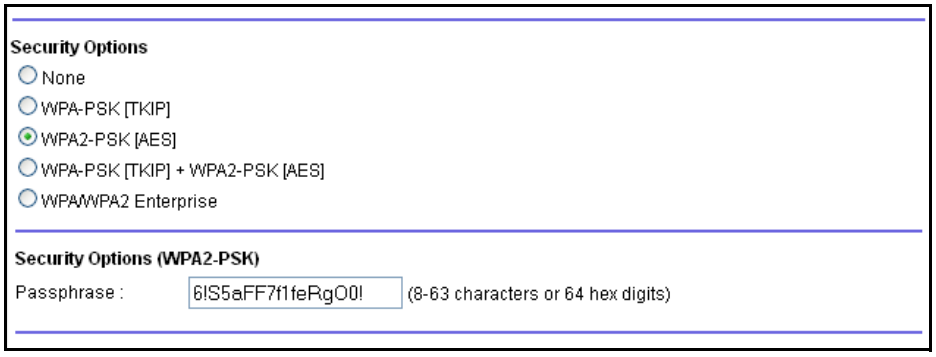
These types of wireless security options use a pre-shared key (PSK), which is the same as a passphrase, wireless network password, or network key.

You can select from the following wireless PSK security options:

- **WPA-PSK [TKIP]**. Wi-Fi Protected Access (WPA) provides strong data security with Temporal Key Integrity Protocol (TKIP) encryption. This option supports speeds of up to 54 Mbps only.
- **WPA2-PSK [AES]**. Wi-Fi Protected Access version 2 (WPA2) provides strong data security with Advanced Encryption Standard (AES) encryption. This is the preset wireless security that is enabled by default. WPA2 provides the most reliable security. This option supports speeds of up to 300 Mbps. If not all clients in your network support WPA2, select WPA-PSK + WPA2-PSK mixed mode.
- **WPA-PSK [TKIP] + WPA2-PSK [AES]**. WPA-PSK + WPA2-PSK is referred to as mixed mode, which supports a combination of TKIP and AES encryption for both WPA and WPA2 clients. For WPA clients, this option supports speeds of up to 54 Mbps only. For WPA2 clients, this option supports speeds of up to 300 Mbps.

➢ **To change the WPA wireless security option and passphrase:**

1. In the Security Options sections of the Wireless Settings screen, select one of the WPA options with PSK.



2. In the associated Passphrase field, enter the passphrase that you want to use.

   The passphrase is a text string from 8 to 63 ASCII characters or exactly 64 hexadecimal digits. A hexadecimal digit is one of the following characters: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, and F.

Wireless clients need to use the passphrase to access the wireless network through the router.

3. Click the **Apply** button.

WPA/WPA2 Enterprise

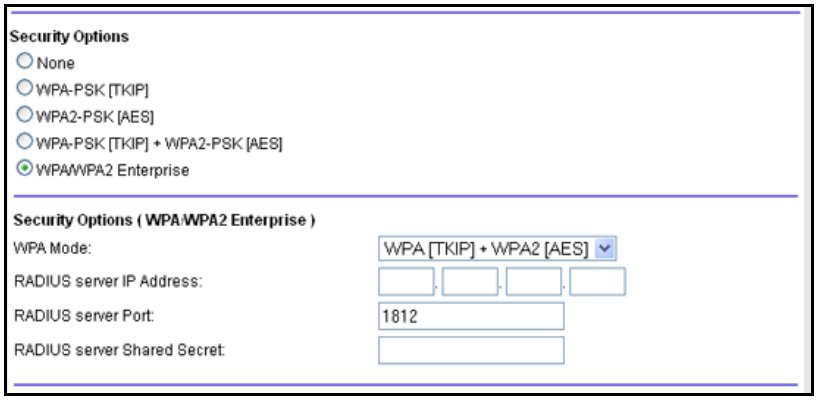
This security option is not for home use but is typically used in a business or enterprise. WPA/WPA2 Enterprise does not use a passphrase but supports 802.1x authentication, which requires an internal or external RADIUS server. A Remote Authentication Dial In User Service (RADIUS) server provides Authentication, Authorization, and Accounting (AAA) management to grant (or deny) computers access to your wireless network.

WPA/WPA2 Enterprise can support WPA [TKIP] for WPA clients only, WPA2 [AES] for WPA2 clients only, and WPA [TKIP] + WPA2 [AES], which is a combination of TKIP and AES encryption for both WPA and WPA2 clients. WPA clients are supported at speeds of up to 54 Mbps only. WPA2 clients are supported at speeds of up 300 Mbps.

WPA/WPA2 Enterprise supports five Extensible Authentication Protocol (EAP) authentication methods: EAP-TLS, EAP-TTLS/MSCHAPv2, PEAPv0/EAP-MSCHAPv2, PEAPv1/EAP-GTC, and EAP-SIM.

➢ **To configure WPA/WPA2 Enterprise security:**

1. In the Security Options sections of the Wireless Settings screen, select the **WPA/WPA2 Enterprise** radio button.



2. Select the WPA mode (**WPA [TKIP]**, **WPA2 [AES]**, or **WPA [TKIP] + WPA2 [AES]**).
3. Type the IP address of the RADIUS server.

   The address can be on your LAN on it can be an external address.
4. Enter the port number for the RADIUS server in the range from 1 to 65535 (the default number is 1812).
5. Type the shared secret, which needs to be between 1 and 128 characters (the default value is blank).

   The shared secret is case-sensitive.
6. Click the **Apply** button.

WEP

Wired Equivalent Privacy (WEP) security is an authentication and data encryption mode that has been superseded by WPA-PSK and WPA2-PSK. WEP supports speeds of up to 54 Mbps (the router is capable of speeds of up 300 Mbps) and does not function with WPS. However, if you set up a wireless distribution system (WDS; see *Wireless Distribution System (WDS)* on page 82), WEP is the only security that can be supported.

Note: The WEP option displays only if you select Up to 54 Mbps from the Mode menu.

➢ **To configure WEP security:**

1. In the Security Options sections of the Wireless Settings screen, select the **WEP** radio button.

2. In the Authentication Type list, select one of the following types:
   - **Automatic**. If you enter a passphrase in the Passphrase field and click the Generate button, the four keys are automatically generated.
   - **Shared Key**. If you select this option, you need to select one key and enter the value manually.
3. In the Encryption Strength list, select the encryption key size:
   - **64-bit**. Standard WEP encryption, using 40/64-bit encryption.
   - **128-bit**. Standard WEP encryption, using 104/128-bit encryption. This selection provides higher encryption security.

4. Depending on the authentication type, generate the key automatically or enter it manually:
   - If the authentication type is Automatic:
     a. In the Passphrase field, enter a passphrase:
     b. Click the **Generate** button.

        For 64-bit WEP, four different WEP keys are generated. For 128-bit WEP, only one WEP key is generated, and the four key fields are populated with the same WEP key.
   - If the authentication type is Shared Key:
     a. Specify the active key by selecting the **Key 1**, **Key 2**, **Key 3**, or **Key 4** radio button.

        Only one key can be the active key.
     b. Enter the value for the key manually:
        - For 64-bit WEP, enter 10 hexadecimal digits (any combination of 0–9, A–F). The key values are not case-sensitive.
        - For 128-bit WEP, enter 26 hexadecimal digits (any combination of 0–9, A–F). The key values are not case-sensitive.
5. Click the **Apply** button.

Attached Devices

➢ **To view all computers and devices, including intruders (unauthorized users) that are currently connected to your wired and wireless networks:**

Select **Basic > Attached Devices**.

The Attached Devices screen displays:

Wired devices are connected to the router through Ethernet cables. Wireless devices have joined the wireless network.

The Wired Devices and Wireless Devices tables show the following information:

- # (number). The order in which the device joined the network.
- **IP Address**. The IP address that the router assigned to this device when it joined the network. Note that this number can change if a device is disconnected and rejoins the network.
- **MAC Address**. The unique MAC address for each device does not change. The MAC address is typically shown on the product label.
- **Device Name**. If the device name is known, it is shown here.

Click the **Refresh** button to update the information onscreen.

Parental Controls

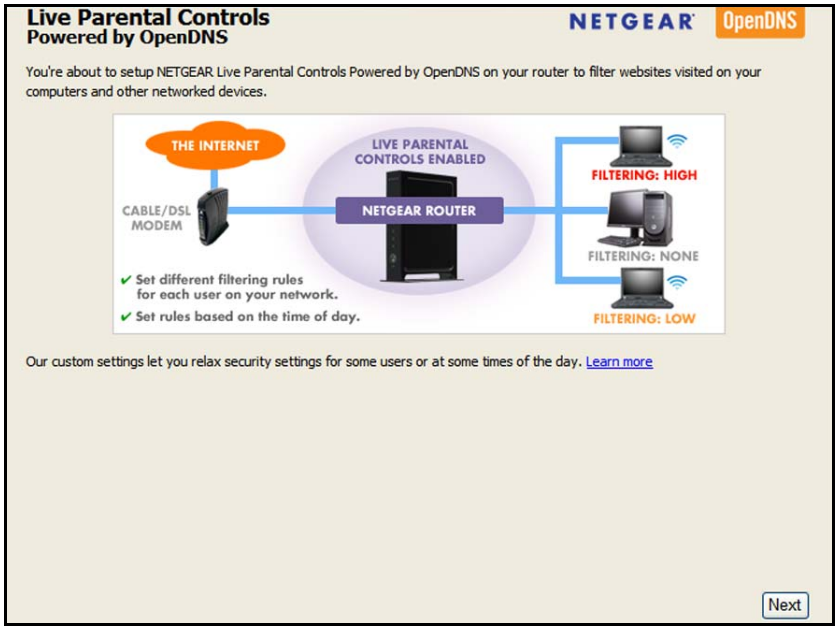
The first time that you select Parental Controls from the Basic Home screen, you are automatically directed to the NETGEAR website where you can learn more about Live Parental Controls or download the application. The following screen displays:

Figure 7. Live Parent Controls screen

➢ **To set up Live Parental Controls:**

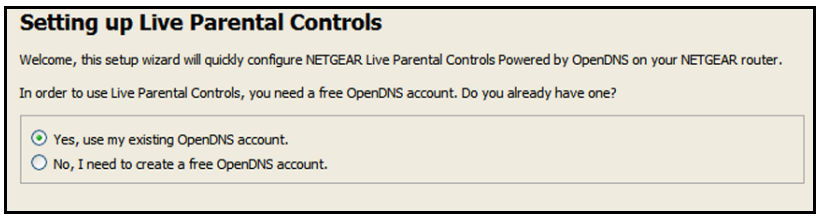
1. On the Live Parental Controls screen, click either the **Windows Users** or **Mac Users** button.
2. Follow the onscreen instructions to download and install the NETGEAR Live Parental Controls Management Utility.

   After installation, Live Parental Controls automatically starts.



3. Click **Next**, read the note, and click **Next** again to proceed.

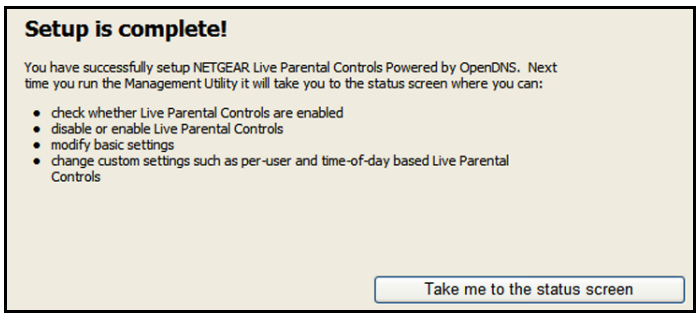
   You are prompted to log in or create a free account.



4. Select the radio button that applies to you and click **Next**.
   - If you already have an OpenDNS account, leave the **Yes** radio button selected.
   - If you do not have an OpenDNS account, select the **No** radio button. A screen displays that lets you set up a free OpenDNS account.

After you log on or create your account, the filtering level screen displays:

5. Select the radio button for the filtering level that you want and click **Next**.



6. Click the **Take me to the status screen** button.

Parental controls are now set up for the router. The dashboard shows Parental Controls as enabled.

The next time that you select Parental Controls on the Basic Home screen, you can sign in to your free OpenDNS account and manage the parental controls.

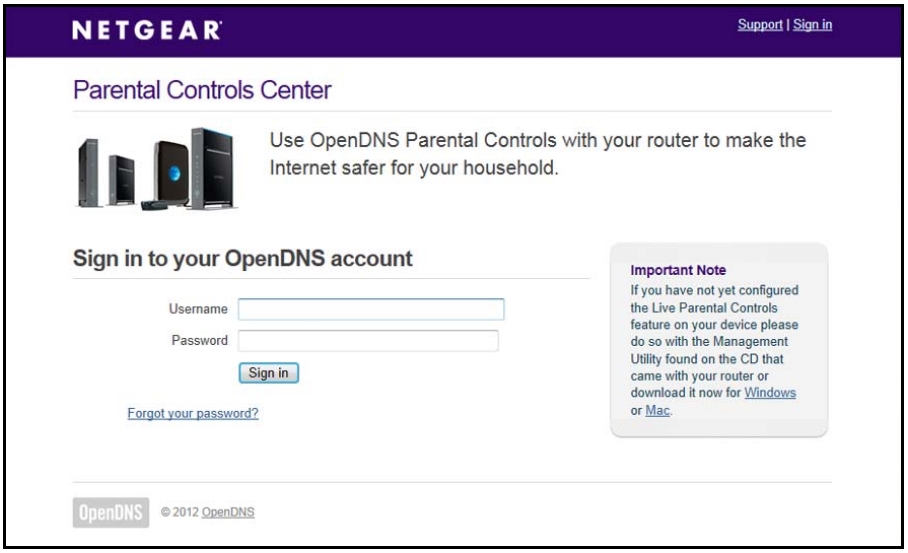


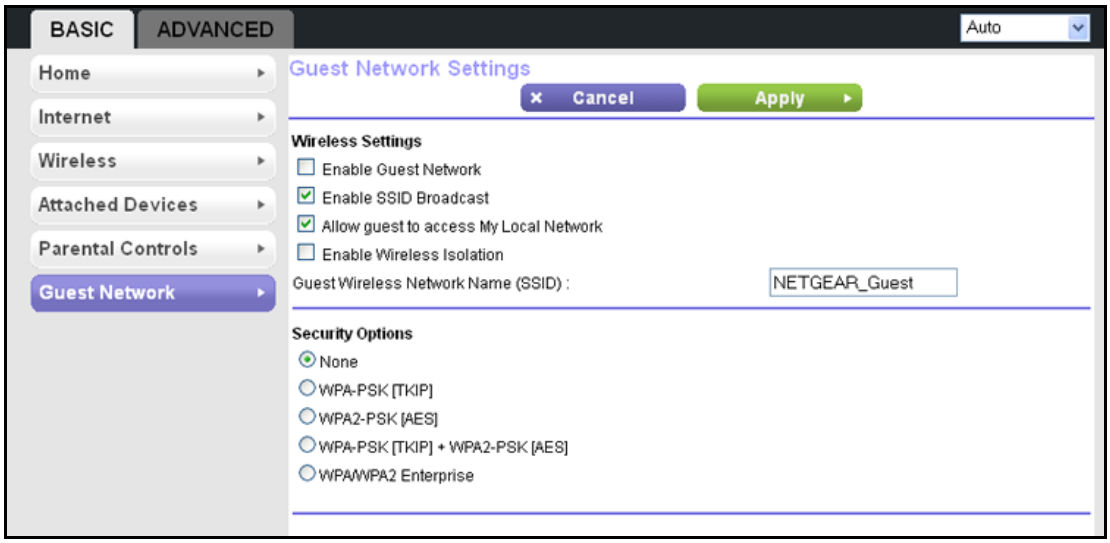
Figure 8. Sign in to your OpenDNS account screen

Guest Network

Adding a wireless guest network allows visitors at your home to use the Internet without seeing your passphrase. You can also specify the degree of access that you give to visitors.

➢ **To set up a guest network:**

1. Select **Basic > Guest Network**.
2. The Guest Network Settings screen displays:



3. Select or clear any of the following optional wireless settings:
   - **Enable Guest Network**. If this check box is selected, the guest network is enabled, and guests can connect to your network using the SSID of this profile. By default, this check box is cleared.
   - **Enable SSID Broadcast**. If this check box is selected, the router broadcasts its SSID to all wireless devices. By default, this check box is selected.
   - **Allow guest to access My Local Network**. If this check box is selected, any user who connects to this SSID has access to your local network, not just Internet access. By default, this check box is selected.
   - **Enable Wireless Isolation**. If this check box is selected, wireless devices that join the network can use the Internet, but cannot access each other or access Ethernet devices on the network. By default, this check box is cleared.
4. Give the guest network a name (SSID).

   The guest network name is case-sensitive and can be up to 32 characters. The default guest SSID is NETGEAR_Guest. This SSID is *in addition* to the regular SSID that you set up on the Wireless Settings screen (see *Wireless Settings Screen Fields* on page 28).

5. Select a security option for the guest network.

   The security options that are available for the wireless guest network are the same options that are available for the regular wireless network (see *WPA-PSK, WPA2-PSK, and WPA-PSK + WPA2-PSK Mixed Mode* on page 29, *WPA/WPA2 Enterprise* on page 30, and *WEP* on page 31).

   By default, the wireless guest network has no security (no authentication or encryption). However, NETGEAR recommends that you do select a security option.

6. Click the **Apply** button.

genie Advanced Home

4

Specify custom settings

This chapter describes the features that are available from the genie Advanced Home screen:

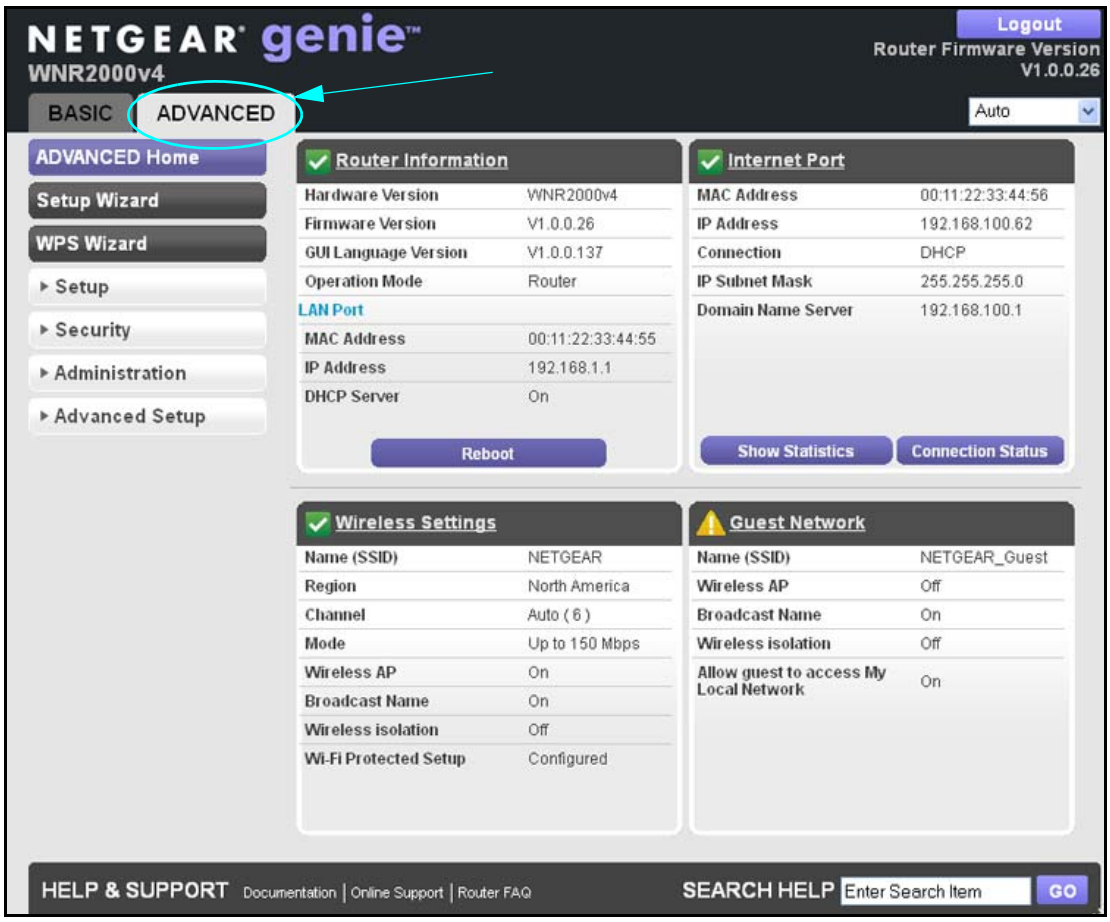


Figure 9. genie Advanced Home screen

This chapter contains the following sections:

- *Setup Wizard*
- *WPS Wizard*
- *Setup Menu*
- *WAN Setup*

- *LAN Setup*
- *QoS Setup*

The following menu selections that you can access from the Advanced Home screen are described in separate chapters:

- **Security**. For information, see *Chapter 5, Security*.
- **Administration**. For information, see *Chapter 6, Administration*.
- **Advanced Setup**. For information, see *Chapter 7, Advanced Settings*.

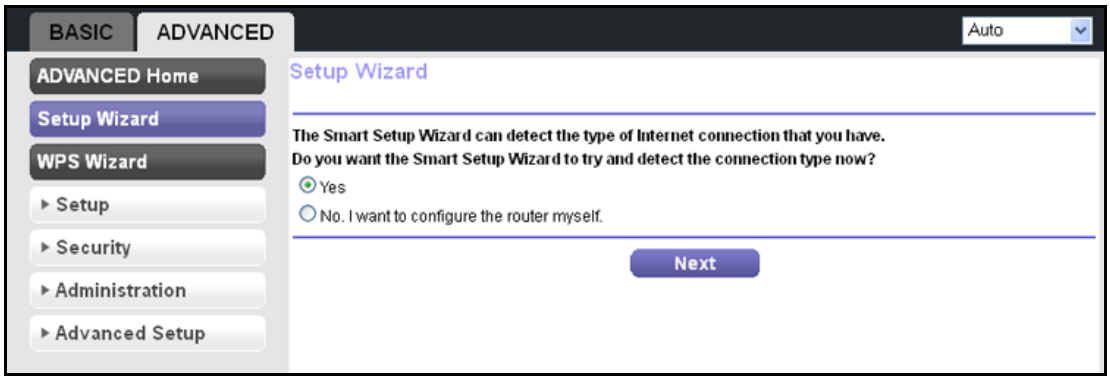
Setup Wizard

The NETGEAR genie installation process is launched with the Setup Wizard the very first time that you start up the router. After you have set up the router, the genie installation process no longer launches automatically, but you can launch the Setup Wizard manually.

➢ **To launch the Setup Wizard:**

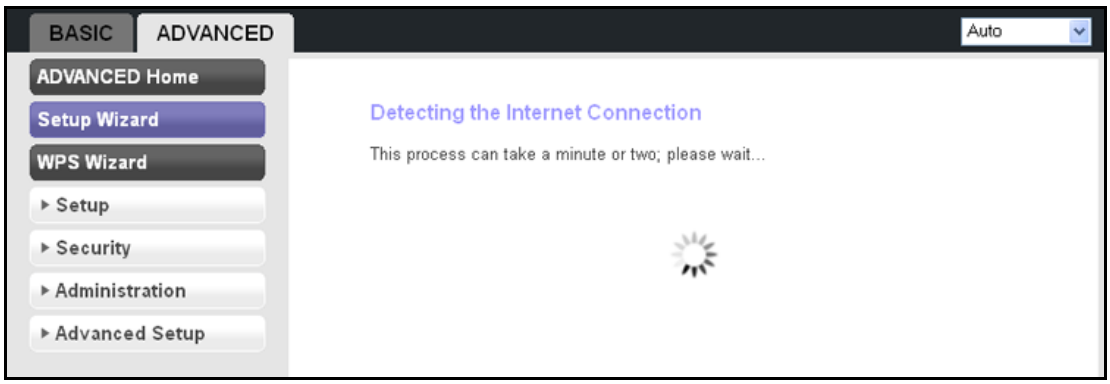
1. Select **Advanced > Setup Wizard**.

   The Setup Wizard screen displays:

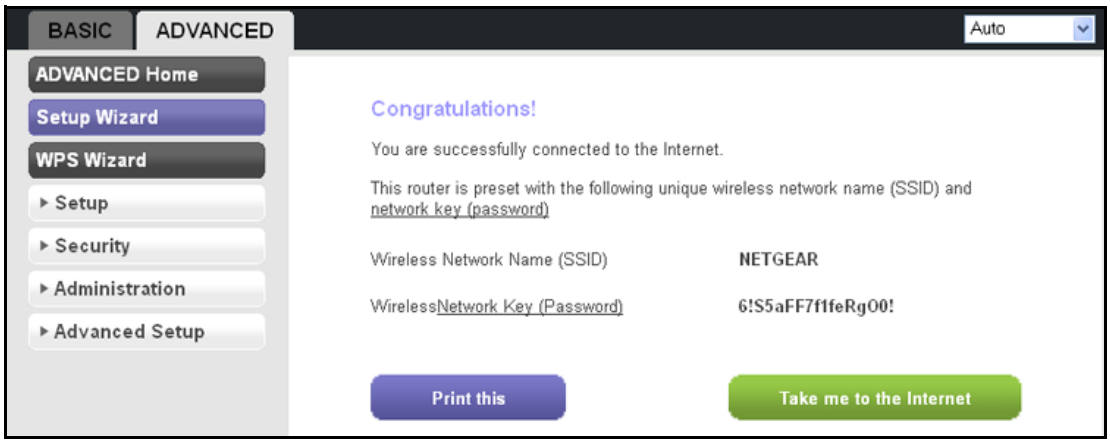


2. Select **Yes**, and click the **Next** button.

   The next screen displays. (If you select the **No, I want to configure the router myself** radio button, the Internet Setup screen displays. The Internet Setup screen is described in *Internet Setup* on page 24.)



The Setup Wizard searches your Internet connection for servers and protocols to determine your ISP configuration. When the Setup Wizard is successful, the following screen displays:



WPS Wizard

The WPS Wizard helps you add a WPS-capable client (a computer or other wireless device) to your network. On the client, you need to either press its WPS button or locate its WPS PIN.

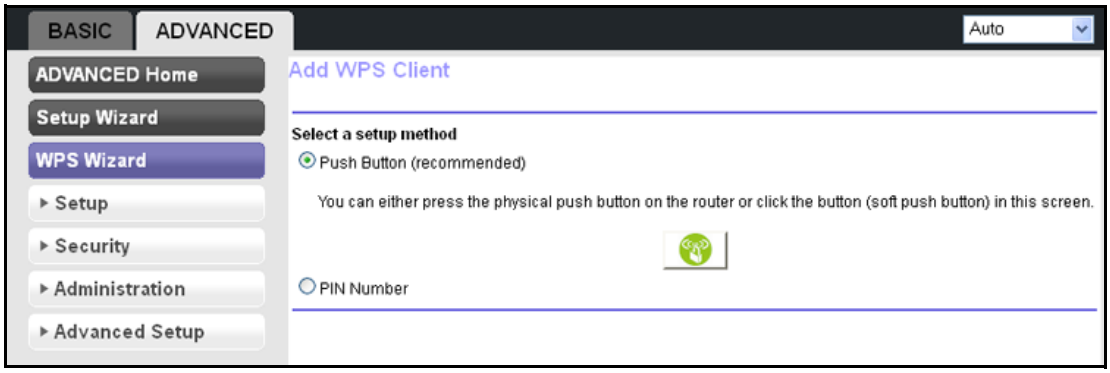
➢ **To use the WPS Wizard:**

1. Select **Advanced > WPS Wizard**.

   The Add WPS Client displays.

2. Click the **Next** button.

   The screen that displays lets you select the method for adding the client:



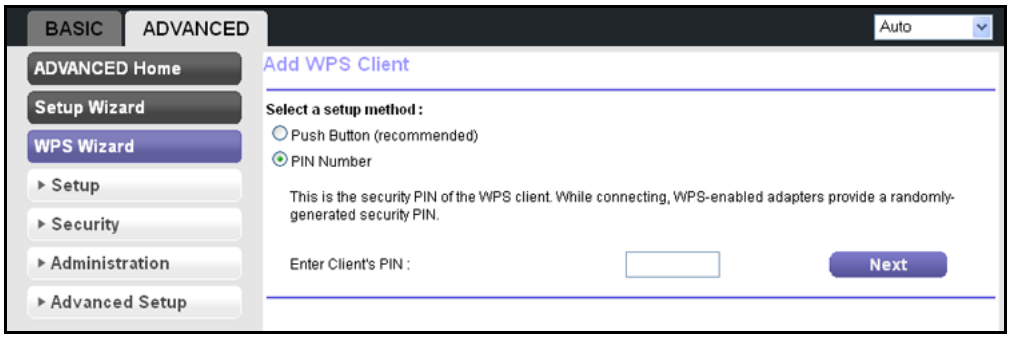
3. Select one of the following options:
   - **Push Button**. To use the push button method, do the following:
     a. Either click the **WPS** radio button on this screen, or press the **WPS** button that is located on the front panel of the router (see *Front Panel* on page 9).
     b. Within 2 minutes, go to the client and press its **WPS** button to let the client join the network.

You do not need to enter a password.

- **PIN Number**. To use the PIN method, do the following:

  a. Select the **PIN Number** radio button.

  The screen adjusts:



  b. Enter the client security PIN.

  c. Click the **Next** button.

  Within 2 minutes, go to the client and use its WPS software to let the client join the network.

  You do not need to enter a password.

  While the router attempts to add the WPS-capable client, the WPS LED on the front of the router blinks green. When the router establishes a WPS connection, the LED is solid green, and the router WPS screen displays a confirmation message.

  d. Repeat this procedure to add another WPS client to your network.

Setup Menu

Select **Advanced > Setup** to display the Setup menu. The following selections are available:

- **Internet Setup**. This is a shortcut to the same Internet Setup screen that you can access from the dashboard on the Basic Home screen. For information, see *Internet Setup* on page 24.
- **Wireless Setup**. This is a shortcut to the same Wireless Settings screen that you can access from the dashboard on the Basic Home screen. For information, see *Basic Wireless Settings* on page 26.
- **Guest Network**. This is a shortcut to the same Guest Network screen that you can access from the dashboard on the Basic Home screen. For information, see *Guest Network* on page 36.
- **WAN Setup**. Internet (WAN) setup. For information, see *WAN Setup* on page 43.
- **LAN Setup**. Local area network (LAN) setup. For information, see *LAN Setup* on page 46.
- **QoS Setup**. Quality of Service (QoS) setup. For information, see *QoS Setup* on page 51.

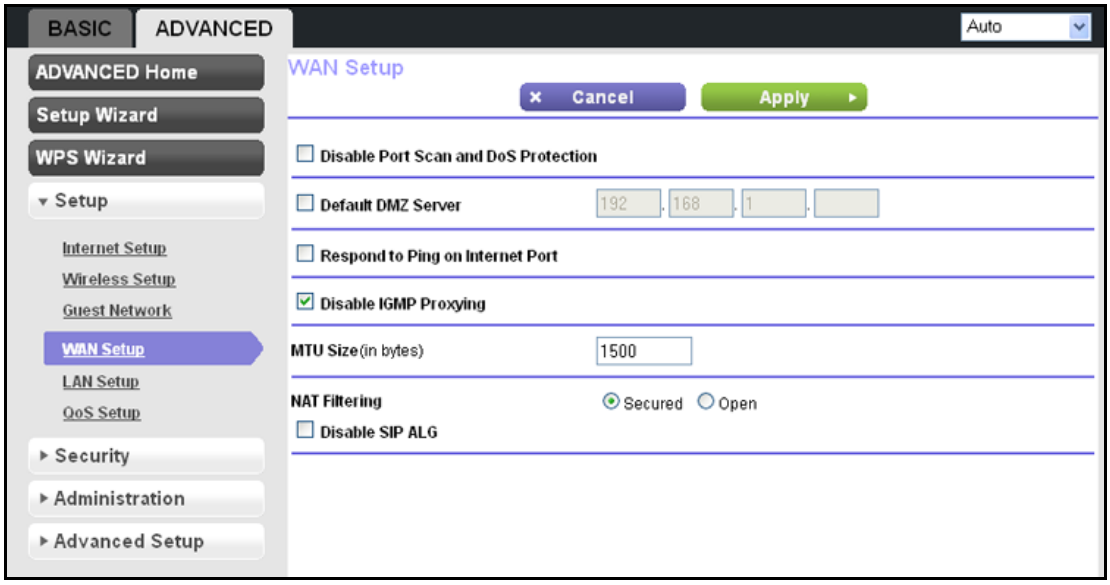
WAN Setup

The WAN Setup screen lets you configure a demilitarized zone (DMZ) server, change the maximum transmit unit (MTU) size, and enable the router to respond to a ping on the Internet (WAN) port.

➢ **To change the WAN settings:**

1. Select **Advanced > Setup > WAN Setup**.

   The WAN Setup screen displays:



2. Enter the settings that you want to customize.

   These settings are described in the following section, *WAN Setup Screen Settings*.

3. Click the **Apply** button.

WAN Setup Screen Settings

The following settings are available on this screen:

Disable Port Scan and DoS Protection. DoS protection protects your LAN against denial of service attacks such as Syn flood, Smurf Attack, Ping of Death, Teardrop Attack, UDP Flood, ARP Attack, Spoofing ICMP, Null Scan, and many others. By default, this check box is cleared.

Default DMZ Server. A demilitarized zone (DMZ) server can be helpful when you play online games and use videoconferencing. Be careful when you use this feature because it makes the firewall security less effective. For more information, see *Default DMZ Server* on page 44.

Respond to Ping on Internet Port. If you want the router to respond to a ping from the Internet, select this check box. By default, the check box is cleared. Use this option only as a

diagnostic tool because it allows your router to be discovered. Do not select this check box unless you have a specific reason.

Disable IGMP Proxying. IGMP proxying allows computers on the LAN to receive the multicast traffic they are subscribed to from the Internet. By default, this check box is selected, and the IGMP proxy is disabled, preventing multicast traffic from the Internet to the LAN. Clear the **Disable IGMP Proxying** check box to allow multicast traffic from the Internet to the LAN.

MTU Size (in bytes). The normal maximum transmit unit (MTU) value for most Ethernet networks is 1500 bytes, or 1492 bytes for PPPoE connections. For some ISPs, you might need to reduce the MTU. This is rarely required, and you should not do this unless you are sure that it is necessary for your ISP connection. For more information, see *Change the MTU Size* on page 45.

NAT Filtering. Network Address Translation (NAT) determines how the router processes inbound traffic:

- Secured NAT provides a secured firewall to protect the computers on the LAN from attacks from the Internet, but might prevent some Internet games, point-to-point applications, or multimedia applications from functioning. By default, the Secured radio button is selected.
- Open NAT provides a much less secured firewall, but allows almost all Internet applications to function.

Disable SIP ALG. Some Voice over IP (VoIP) applications do not function well with the Session Initiation Protocol (SIP) Application Layer Gateway (ALG). Selecting the check box to turn off the SIP ALG might enable connected VoIP devices to create and accept a VoIP call through the router. By default, the check box is cleared.

Default DMZ Server

The default DMZ server feature is helpful when you use some online games and videoconferencing applications that are incompatible with Network Address Translation (NAT). The router is programmed to recognize some of these applications and to function correctly with them, but there are other applications that might not function well. In some cases, one local computer can run the application correctly if that computer's IP address is entered as the default DMZ server.

WARNING:

DMZ servers pose a security risk. A computer designated as the default DMZ server loses much of the protection of the firewall and is exposed to exploits from the Internet. If compromised, the DMZ server computer can be used to attack other computers on your network.

Incoming traffic from the Internet is usually discarded by the router unless the traffic is a response to one of your local computers or a service that you have configured on the Port Forwarding / Port Triggering screen (see *Set Up Port Forwarding to Local Servers* on page 90 and *Set Up Port Triggering* on page 93). Instead of discarding this traffic, you can have it forwarded to one computer on your network. This computer is called the default DMZ server.

➢ **To set up a default DMZ server:**

1. Select **Advanced > Setup > WAN Setup**.

   The WAN Setup screen displays.

2. Select the **Default DMZ Server** check box.
3. Type the IP address.
4. Click the **Apply** button.

Change the MTU Size

The maximum transmission unit (MTU) is the largest data packet a network device transmits. When one network device communicates across the Internet with another, the data packets travel through many devices along the way. If any device in the data path has a lower MTU setting than the other devices, the data packets have to be split or fragmented to accommodate the device with the smallest MTU.

The best MTU setting for NETGEAR equipment is often just the default value, and changing the value might fix one problem but cause another.

WARNING:

An incorrect MTU setting can cause Internet communication problems such as the inability to access certain websites, frames within websites, secure login pages, or FTP or POP servers.

Leave MTU unchanged unless one of these situations occurs:

- You have problems connecting to your ISP or other Internet service, and technical support of either the ISP or NETGEAR recommends changing the MTU setting. These web-based applications might require an MTU change:
  - A secure website that does not open, or displays only part of a web page
  - Yahoo email
  - MSN portal
  - America Online’s DSL service
- You use VPN and have severe performance problems.
- You used a program to optimize MTU for performance reasons, and now you have connectivity or performance problems.

If you suspect an MTU problem, a common solution is to change the MTU to 1400. If you are willing to experiment, you can gradually reduce the MTU from the maximum value of 1500 until the problem goes away.

The following table describes common MTU sizes and applications.

Table 3. Common MTU sizes

MTU	Application
1500	The largest Ethernet packet size and the default value. This is the typical setting for non-PPPoE, non-VPN connections, and is the default value for NETGEAR routers, adapters, and switches.
1492	Used in PPPoE environments.
1472	Maximum size to use for pinging. (Larger packets are fragmented.)
1468	Used in some DHCP environments.
1460	Usable by AOL if you do not have large email attachments, for example.
1436	Used in PPTP environments or with VPN.
1400	Maximum size for AOL DSL.
576	Typical value to connect to dial-up ISPs.

➢ **To change the MTU size:**

1. Select **Advanced > Setup > WAN Setup**.

   The WAN Setup screen displays.

2. In the MTU Size field, enter a new size between 64 and 1500.
3. Click the **Apply** button.

LAN Setup

The LAN Setup screen allows configuration of LAN IP services such as Dynamic Host Configuration Protocol (DHCP) and Routing Information Protocol (RIP).

The router is shipped preconfigured to use private IP addresses on the LAN side and to function as a DHCP server. The router's default LAN IP configuration is:

- LAN IP address. **192.168.1.1**
- Subnet mask. **255.255.255.0**

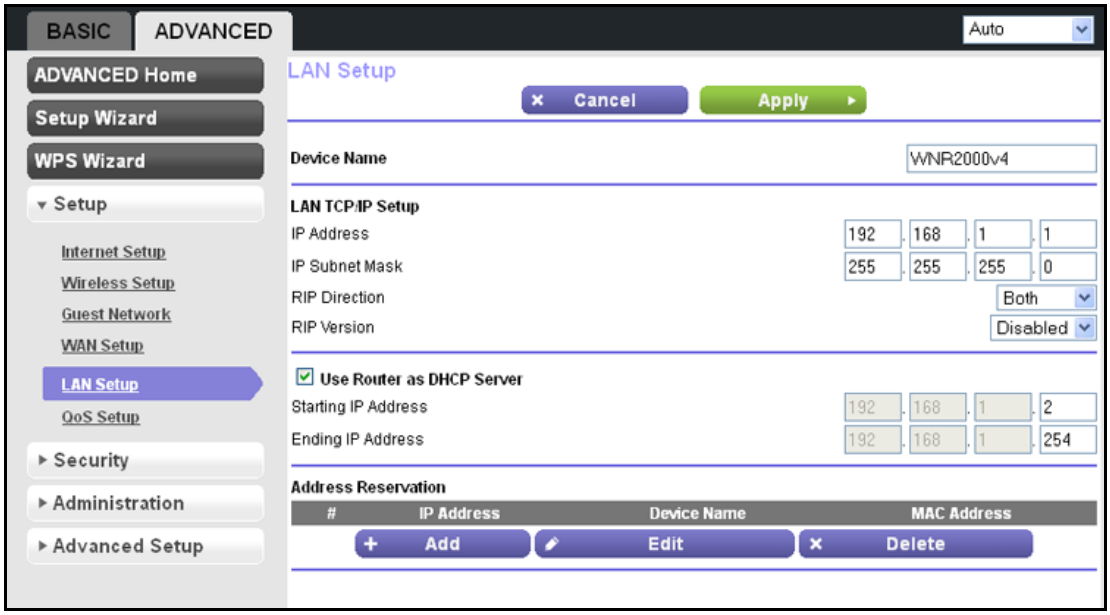
These addresses are part of the designated private address range for use in private networks and should be suitable for most applications. If your network has a requirement to use a different IP addressing scheme, you can make those changes on the LAN Setup screen.

Note: If you change the LAN IP address of the router while connected through the browser, you are disconnected. If this situation occurs, you need to open a new connection to the new IP address and log in again.

➢ **To change the LAN settings:**

1. Select **Advanced > Setup > LAN Setup**.

   The LAN Setup screen displays:



2. Enter the settings that you want to customize.

   These settings are described in the following section, *LAN Setup Screen Settings*.

3. Click the **Apply** button.

LAN Setup Screen Settings

The following settings are available on this screen:

LAN TCP/IP Setup

IP Address. The LAN IP address of the router (by default, 192.168.1.1).

IP Subnet Mask. The LAN subnet mask of the router (by default, 255.255.255.0). Combined with the IP address, the IP subnet mask allows a device to know which other addresses are local to it, and which have to be reached through a gateway or router.

RIP Direction. Router Information Protocol (RIP) enables a router to exchange routing information with other routers. This setting controls how the router sends and receives RIP packets. Both is the default setting. With the Both or Out Only setting, the router broadcasts

its routing table periodically. With the Both or In Only setting, the router incorporates the RIP information that it receives.

RIP Version. This controls the format and the broadcasting method of the RIP packets that the router sends. It recognizes both formats when receiving. By default, the RIP function is disabled. There are three RIP versions:

- RIP-1 is universally supported. It is adequate for most networks, unless you have an unusual network setup.
- RIP-2 carries more information. Both RIP-2B and RIP-2M send the routing data in RIP-2 format:
- RIP-2B uses subnet broadcasting.
- RIP-2M uses multicasting.

Use Router as a DHCP Server

By default, this check box is selected so that the router functions as a Dynamic Host Configuration Protocol (DHCP) server.

Starting IP Address. Specify the start of the range for the pool of IP addresses in the same subnet as the router. The default starting IP address is 192.168.1.2.

Ending IP Address. Specify the end of the range for the pool of IP addresses in the same subnet as the router. The default ending IP address is 192.168.1.254.

For more information, see *Manage the DHCP Server on the Router* on page 48.

Address Reservation

When you specify a reserved IP address for a computer on the LAN, that computer receives the same IP address each time it accesses the router's DHCP server. Assign reserved IP addresses to servers that require permanent IP settings. For more information, see *Set Up Address Reservation* on page 49.

Manage the DHCP Server on the Router

By default, the router functions as a DHCP server, enabling it to assign IP, DNS server, and default gateway addresses to all computers and devices that are connected to the router's LAN. The assigned default gateway address is the LAN address of the router. The router assigns IP addresses to the attached computers and devices from a pool of addresses specified on the LAN Setup screen. Each pool address is tested before it is assigned to avoid duplicate addresses on the LAN. For most applications, the default DHCP and TCP/IP settings of the router function well.

You can specify the pool of IP addresses to be assigned by setting the starting IP address and ending IP address. These addresses should be part of the same IP address subnet as the router's LAN IP address. Using the default addressing scheme, the default range is 192.168.1.2–192.168.1.254, although you might want to save part of this range for devices with fixed addresses.

The router delivers the following parameters to any LAN device that requests DHCP information:

- IP address from the range that you have defined
- Subnet mask
- Gateway IP address (the router's LAN IP address)
- Primary DNS server address (if you entered a primary DNS address on the Internet Setup screen; otherwise, the router's LAN IP address)
- Secondary DNS server address (if you entered a secondary DNS address in the Internet Setup screen)

➢ **To use another device on your network as the DHCP server, or to manually configure the network settings of all of your computers and devices:**

1. Select **Advanced > Setup > LAN Setup**.

   The LAN Setup screen displays.

2. Clear the **Use Router as DHCP Server** check box.
3. Click the **Apply** button.

If the DHCP service is not enabled on the router and no other DHCP server is available on your network, you need to set your computers' IP addresses manually or your computers are not able to access the router.

Set Up Address Reservation

When you specify a reserved IP address for a computer or device on the LAN, that computer or device always receives the same IP address each time it accesses the router's DHCP server. Reserved IP addresses should be assigned to computers or servers that require permanent IP settings.

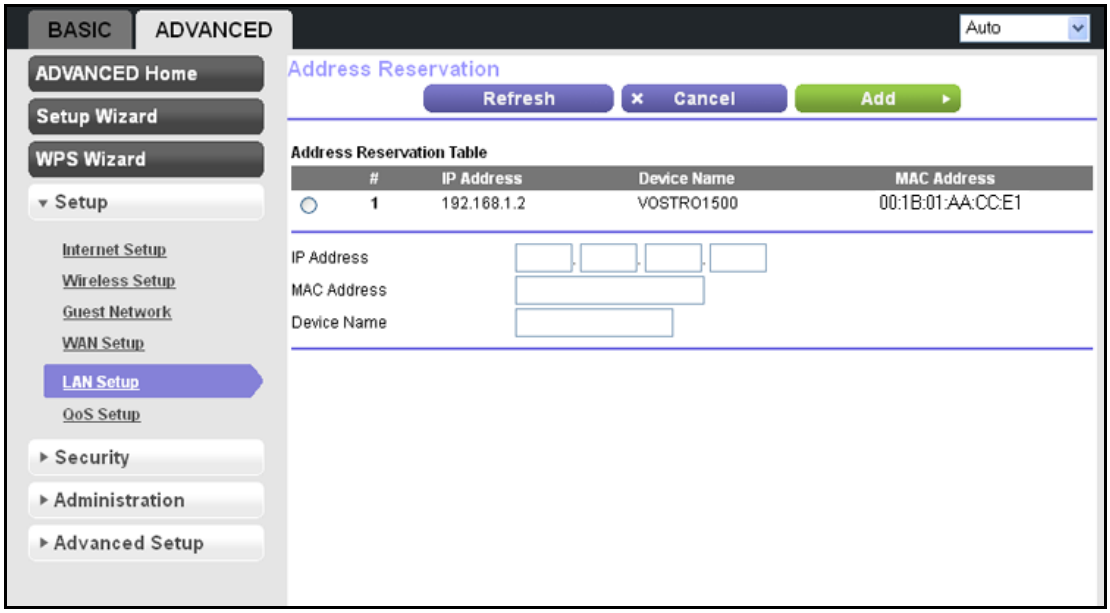
➢ **To reserve an IP address:**

1. Select **Advanced > Setup > LAN Setup**.

   The LAN Setup screen displays.

2. In the Address Reservation section of the screen, click the **Add** button.

The Address Reservation screen displays:



3. In the IP Address field, type the IP address to assign to the computer or server. (Choose an IP address from the router's LAN subnet, such as 192.168.1.x.)

   Tip: If the computer is already on your network, you can select the associated radio button in the Address Reservation table. The computer's information is automatically copied into the IP Address, MAC Address, and Device Name fields.

4. Type the MAC address of the computer or server.
5. Type a name for the computer or server.
6. Click the **Add** button to add the address to the Address Reservation table on the LAN Setup screen.

   The reserved address is not assigned until the next time the computer contacts the router's DHCP server. Reboot the computer or access its IP configuration and force a DHCP release and renew.

➢ **To edit or delete a reserved address entry:**

1. Select **Advanced > Setup > LAN Setup**.

   The LAN Setup screen displays.

2. In the Address Reservation table, select the radio button next to the address that you want to edit or delete.

3. Do one of the following:
   - Click the **Edit** button.

     The Address Reservation screen displays.

     a. Edit the address information.

     b. Click the **Apply** button.
   - Click the **Delete** button.

     The address is removed from the table.

QoS Setup

Quality of Service (QoS) is an advanced feature that you can use to prioritize some types of traffic ahead of others. The router can provide QoS prioritization over the wireless link and on the Internet connection. You use the QoS Setup screen to set up QoS features.

The following sections describe the QoS features.

Wi-Fi Multimedia Quality of Service for Wireless Traffic

The router supports Wi-Fi Multimedia Quality of Service (WMM QoS) to prioritize wireless voice and video traffic over the wireless link. WMM QoS provides prioritization of wireless data packets from different applications based on four access categories: voice, video, best effort, and background. For an application to receive the benefits of WMM QoS, both it and the client running that application need to have WMM enabled. Legacy applications that do not support WMM and applications that do not require QoS are assigned to the best effort category, which receives a lower priority than voice and video.

WMM QoS is enabled by default, and the Enable WMM (Wi-Fi multimedia) settings check box is selected. NETGEAR recommends that you leave this setting as it is for full 802.11n wireless rate support. You can disable it in the QoS Setup screen by clearing this check box and clicking the Apply button.

Quality of Service Priority Rules and Internet Access

You can give prioritized Internet access to the following types of traffic:

- Specific applications
- Specific online games
- Individual Ethernet LAN ports of the router
- A specific device by MAC address

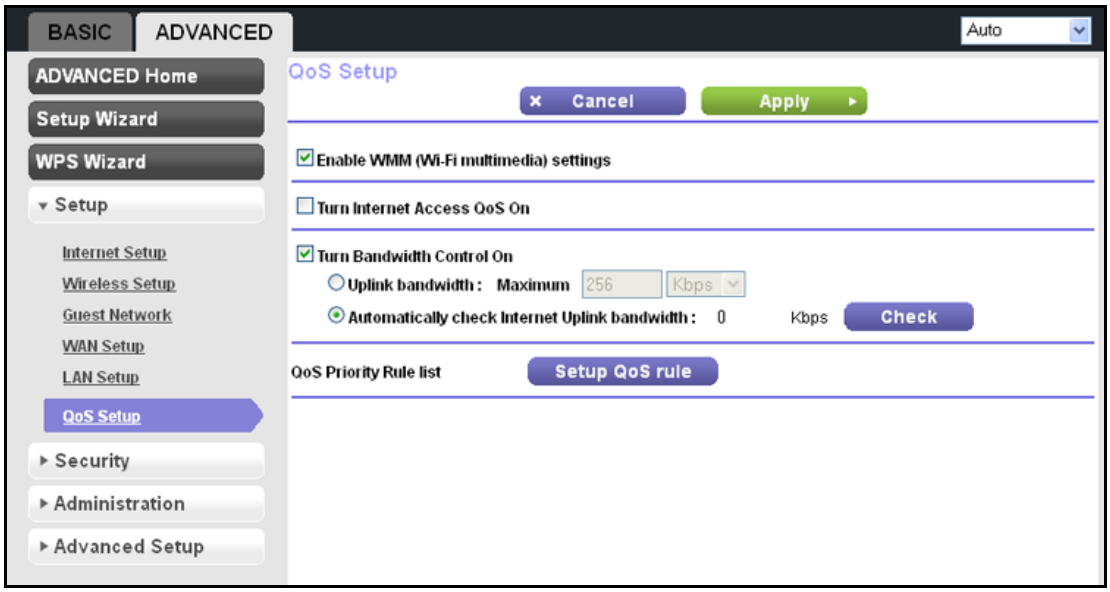
To specify prioritization of traffic, you need to create a policy for the type of traffic and add the policy to the QoS Policy table in the QoS Setup screen. For convenience, the QoS Policy table lists many common applications and online games that can benefit from QoS handling.

By default, QoS is disabled for Internet traffic, the default QoS rules and any custom QoS rules that you created are not activated, and no traffic is prioritized.

➤ **To enable QoS for Internet traffic and activate the QoS rules:**

1. Select **Advanced > Setup > QoS Setup**.

   The QoS Setup screen displays:



2. Select the **Turn Internet Access QoS On** check button.
3. Click the **Apply** button.

The following sections describe how to manage and create QoS rules, which are also referred to as QoS policies.

Manage QoS Rules

The following procedure refers to preconfigured and custom QoS rules. For information about how to create custom QoS rules, see the sections following this section.

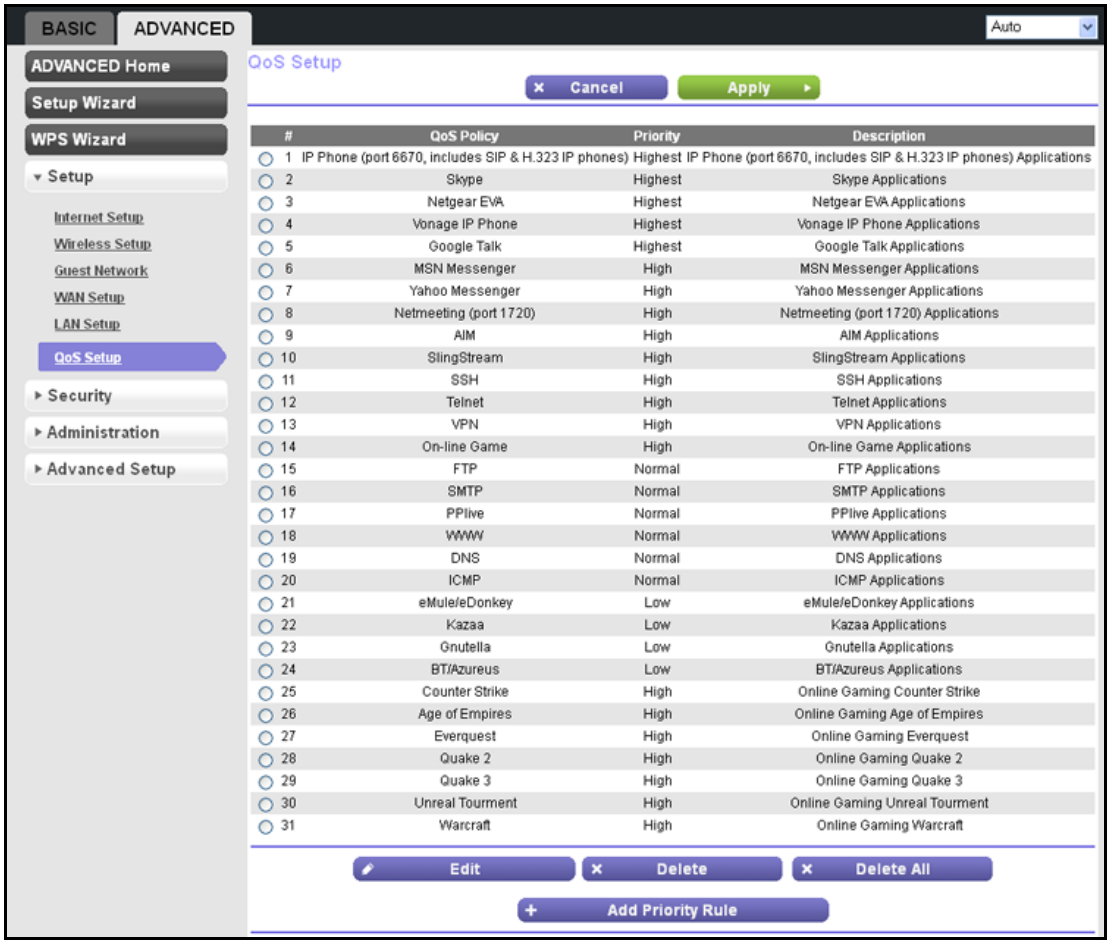
➤ **To view, change, or delete a QoS rule:**

1. Select **Advanced > Setup > QoS Setup**.

   The QoS Setup screen displays.

2. Click the **Setup QoS rule** button.

All preconfigured QoS rules are displayed in a table, along with their priority (Highest, High, Normal, or Low) and a description:



3. Select the radio button next to the QoS policy that you want to edit or delete, and do one of the following:
   - Click the **Delete** button to remove the QoS policy from the table.
   - Click the **Edit** button to edit the QoS policy.

     The QoS - Priority Rules screen displays.

     a. Follow the instructions in the following sections to change the policy settings.
     b. When you are done, click the **Apply** button on the QoS - Priority Rules screen.

        Your changes are saved in the table on the QoS Setup screen.

WARNING:

If you click the Delete All button, *all* preconfigured and custom QoS rules are deleted.

Create a QoS Rule for an Application or Online Game

➢ **To create a QoS policy for an application or online game:**

1. Select **Advanced > Setup > QoS Setup**.

   The QoS Setup screen displays.

2. Click the **Setup QoS rule** button.

   The existing QoS rules display.

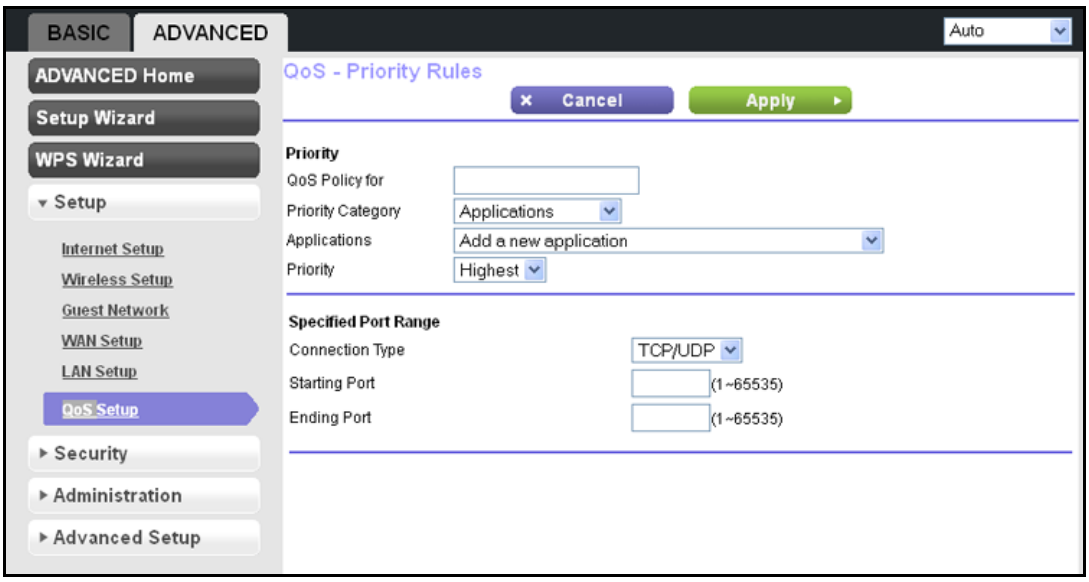
3. Click the **Add Priority Rule** button.

   The QoS - Priority Rules screen displays.

4. In the Priority Category list, select either **Applications** or **Online Gaming**:

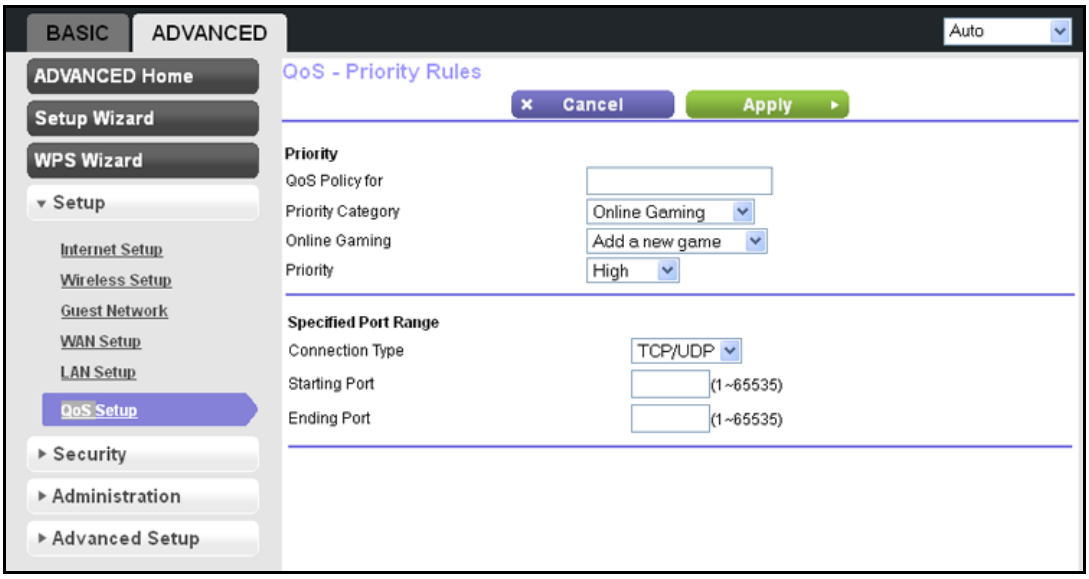
   - **Applications**. The Applications list lets you select existing applications, but scroll down to the bottom to select **Add a new application**.

     The screen adjusts:



   - **Online Gaming**. The Online Gaming list lets you select existing games, but scroll down to the bottom to select **Add a new game**.

The screen adjusts:



5. In the QoS Policy for field, type a descriptive name for the new application or game.
6. From the Priority list, select the priority that this traffic should receive relative to other applications and traffic when accessing the Internet. Select **Highest**, **High**, **Normal**, or **Low**.
7. In the Connection Type field, select either **TCP**, **UDP**, or **TCP/UDP**.
8. In the Starting Port and Ending Port fields, specify the port number or range of port numbers that is used by the application or game.
9. Click the **Apply** button on the QoS - Priority Rules screen.

   The rule is saved in the QoS policy table on the QoS Setup screen.

Create a QoS Rule for a Router LAN Port

➢ **To create a QoS policy for a device connected to one of the router's LAN ports:**

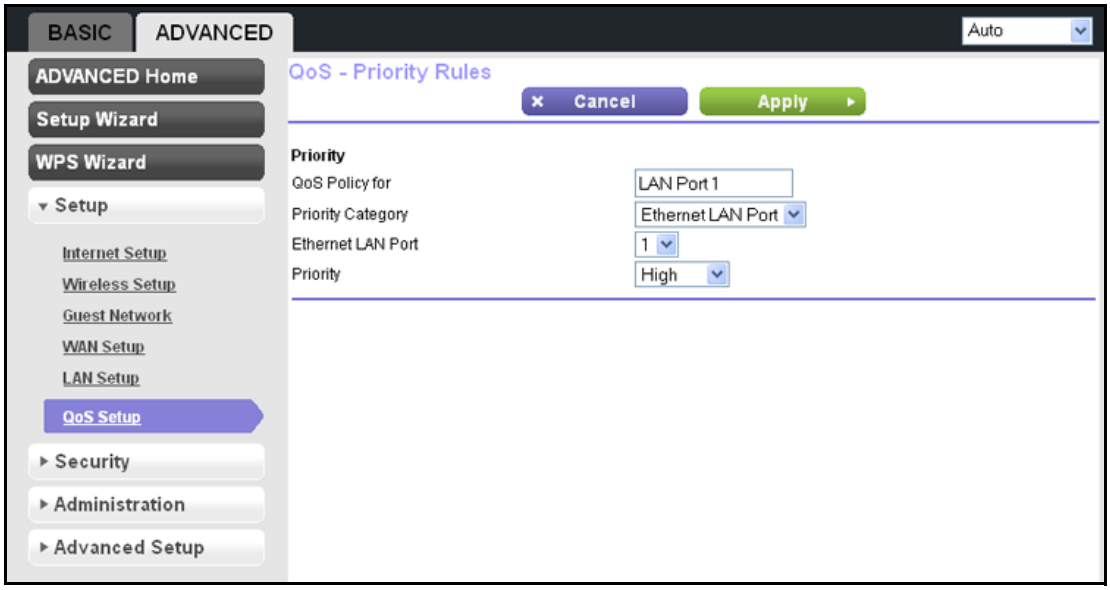
1. Select **Advanced > Setup > QoS Setup**.

   The QoS Setup screen displays.
2. Click the **Setup QoS rule** button.

   The existing QoS rules display.
3. Click the **Add Priority Rule** button.

   The QoS - Priority Rules screen displays.
4. In the Priority Category list, select **Ethernet LAN Port**.

The screen adjusts:



5. From the Ethernet LAN port list, select the LAN port (**1**, **2**, **3**, or **4**) for which you want to configure the QoS policy.
6. From the Priority list, select the priority that this traffic should receive relative to other applications and traffic when accessing the Internet. Select **Highest**, **High**, **Normal**, or **Low**.
7. Click the **Apply** button on the QoS - Priority Rules screen.

   The rule is saved in the QoS policy table on the QoS Setup screen.

Create a QoS Rule for a MAC Address

➢ **To create a QoS policy for traffic from a specific MAC address:**

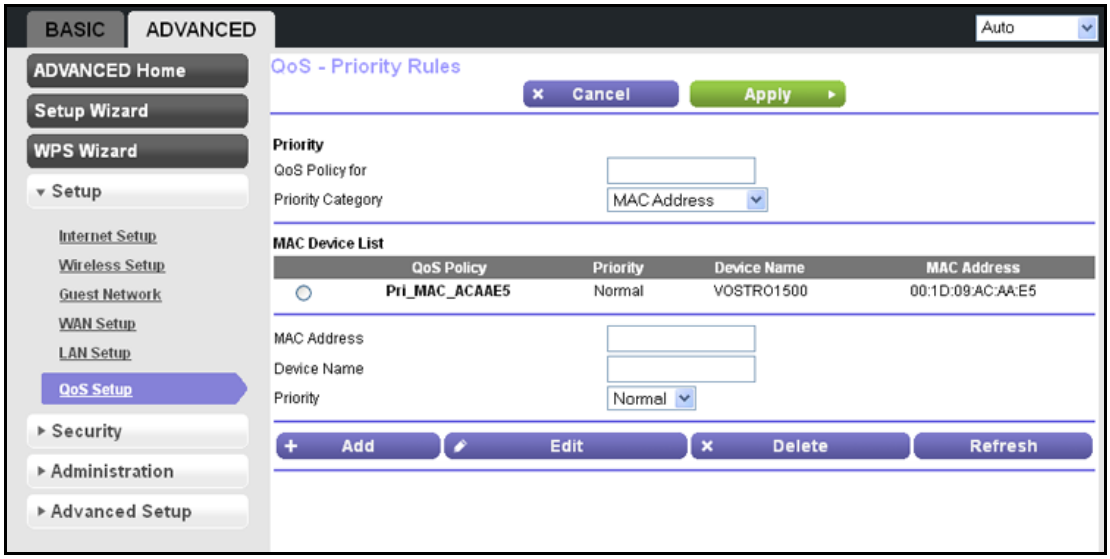
1. Select **Advanced > Setup > QoS Setup**.

   The QoS Setup screen displays.
2. Click the **Setup QoS rule** button.

   The existing QoS rules display.
3. Click the **Add Priority Rule** button.

   The QoS - Priority Rules screen displays.
4. In the Priority Category list, select **MAC Address**.

The screen adjusts:



5. If the device for which you want to create a QoS policy is displayed in the MAC Device List, select its radio button.

   The information from the MAC Device List populates the policy name, MAC Address, and Device Name fields.

6. (Optional) If the device does not appear in the MAC Device List, click the **Refresh** button.

   If it still does not appear, you have to complete these fields manually.

7. From the Priority list, select the priority that this traffic should receive relative to other applications and traffic when accessing the Internet. Select **Highest**, **High**, **Normal**, or **Low**.
8. Click the **Apply** button on the QoS - Priority Rules screen.

   The rule is saved in the QoS policy table on the QoS Setup screen.

➢ **To edit or delete a MAC address on the MAC Device List:**

1. Select **Advanced > Setup > QoS Setup**.

   The QoS Setup screen displays.

2. Click the **Setup QoS rule** button.

   The existing QoS rules display.

3. Click the **Add Priority Rule** button.

   The QoS - Priority Rules screen displays.

4. In the Priority Category list, select **MAC Address**.

   The MAC Device List displays.

5. Select the radio button next to the device that you want to edit or delete, and do one of the following:
   - Click the **Delete** button to remove the device from the table.
   - Click the **Edit** button to edit the MAC address, device name, or priority.

   Note: *You cannot delete or edit a device that was detected by the router and automatically added to the MAC Device List.*

6. Click the **Apply** button on the QoS - Priority Rules screen.

   The device information is saved or removed from the MAC Device List.

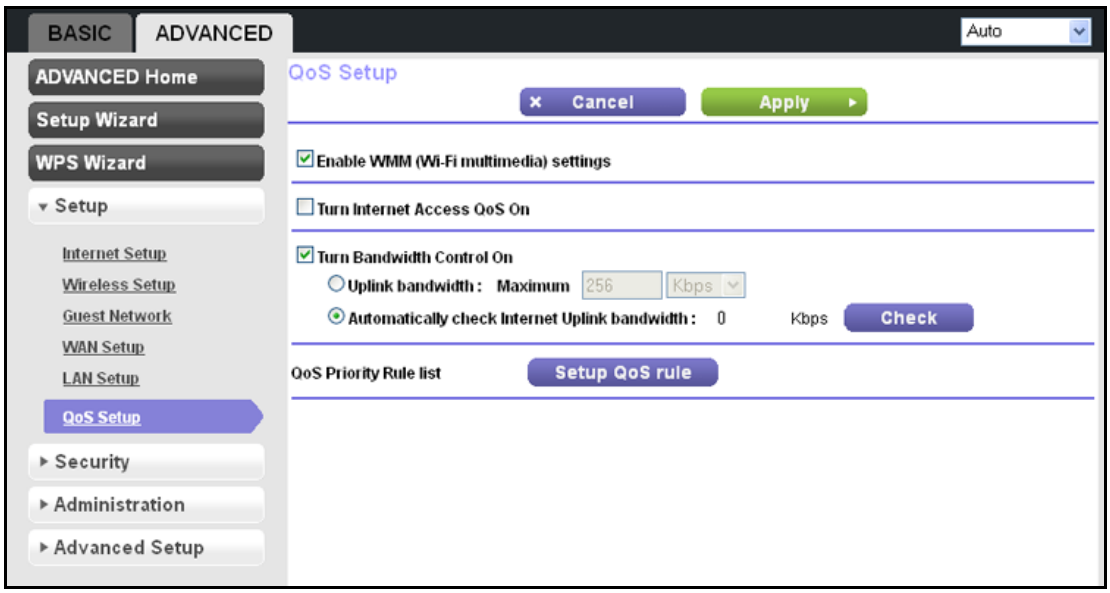
Bandwidth Control

Bandwidth control lets you set a limit to the bandwidth that is available for traffic from the router to the Internet.

➢ **To set the maximum uplink bandwidth:**

1. Select **Advanced > Setup > QoS Setup**.

   The QoS Setup screen displays:



2. Select the **Turn Bandwidth Control On** check box.
3. Select the **Automatically check Internet Uplink bandwidth** radio button.
4. Click the **Check** button.

   The router detects the available uplink bandwidth. After about 1 minute, the available bandwidth displays onscreen. This information can help you to determine the maximum bandwidth setting that you want to allow.

5. Select the **Uplink bandwidth** radio button.

6. Enter the maximum bandwidth that you want to allow, and select either **Kbps** or **Mbps**.
7. Click the **Apply** button.

Security

5

Keep unwanted content out of your network

This chapter explains how to use the basic firewall features of the router to prevent objectionable content from reaching the computers and other devices connected to your network.

This chapter includes the following sections:

- *Keyword Blocking of HTTP Traffic*
- *Block Services (Port Filtering)*
- *Schedule Blocking*
- *Security Event Email Notifications*

Note: For information about parental controls, see *Parental Controls* on page 33.

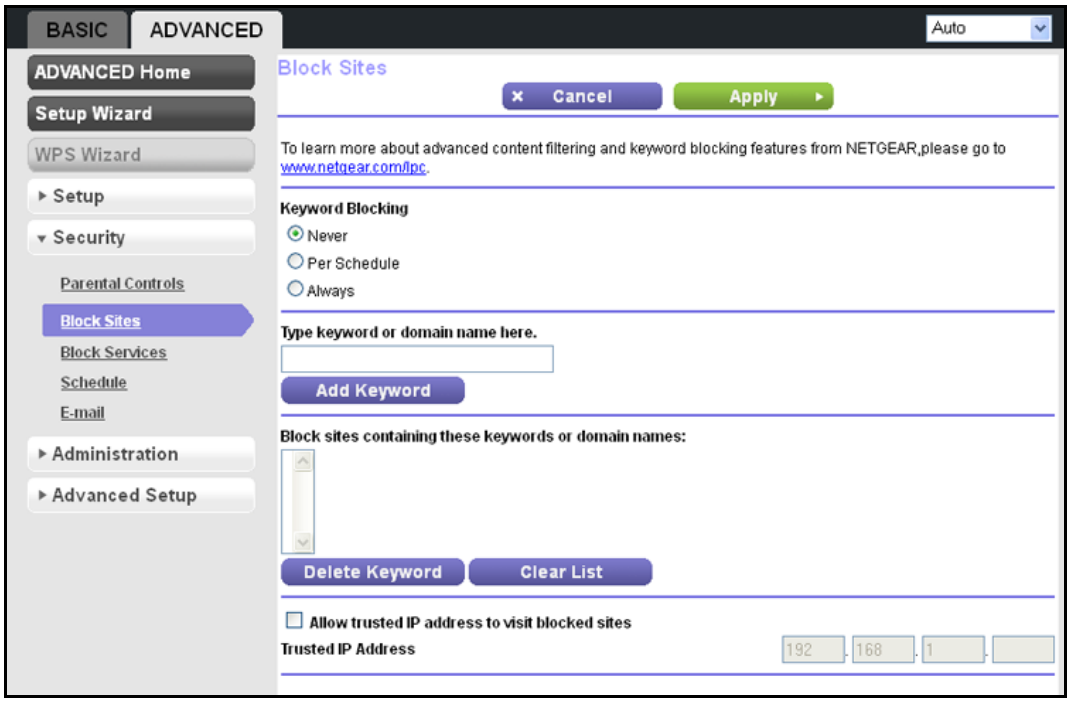
Keyword Blocking of HTTP Traffic

Use keyword blocking to prevent certain types of HTTP traffic from accessing your network. The blocking can be always or according to a schedule.

➢ **To set up keyword blocking:**

1. Select **Advanced > Security > Block Sites**.

   The Block Sites screen displays:



2. Select one of the keyword blocking options (by default, Never is selected):
   - **Per Schedule**. Turn on keyword blocking according to the settings on the Schedule screen (see *Schedule Blocking* on page 65).
   - **Always**. Turn on keyword blocking all the time, independent of the settings on the Schedule screen.
3. In the Type keyword or domain name here field, enter a keyword or domain, and click the **Add Keyword** button.

   Repeat this step to add more keywords or domains.

   The Keyword list supports up to 32 entries. Here are some sample entries:

   - If the keyword xxx is specified, the URL www.zzyyqq.com/xxx.html is blocked, as is the newsgroup alt.pictures.xxx.
   - If the keyword .com is specified, only websites with other domain suffixes (such as .edu or .gov) can be viewed.
   - If a period (.) is specified as the keyword, all Internet browsing access is blocked.
4. Click the **Apply** button.

➢ **To delete a keyword or domain:**

1. Select **Advanced > Security > Block Sites**.

   The Block Sites screen displays.

2. Select the keyword or domain that you want to delete from the list.
3. Click the **Delete Keyword** button.

   Clicking the Clear List button deletes all keywords and domains from the list.

4. Click the **Apply** button.

> **Note:** If you have set up email notifications (see *Security Event Email Notifications* on page 66), you can be notified when someone attempts to access a blocked site.

Exempt a Computer from Blocking and Logging

You can exempt one trusted computer from blocking and logging. The computer you exempt needs to have a fixed IP address.

➢ **To specify a trusted computer:**

1. Select **Advanced > Security > Block Sites**.

   The Block Sites screen displays.

2. Select the **Allow trusted IP address to visit blocked sites** radio button.
3. In the Trusted IP Address field, type the last octet of the IP address.

   The first three octets of the IP address depend on the IP address that is assigned to the router on the LAN Setup screen.

4. Click the **Apply** button.

Block Services (Port Filtering)

Services are functions performed by server computers at the request of client computers. For example, web servers serve web pages, time servers serve time and date information, and game hosts serve data about other players' moves. When a computer on the Internet sends a request for service to a server computer, the requested service is identified by a service or port number. This number appears as the destination port number in the transmitted IP packets. For example, a packet that is sent with the destination port number 80 is an HTTP (web server) request.

The service numbers for many common protocols are defined by the Internet Engineering Task Force (IETF at *http://www.ietf.org/*) and published in RFC1700, "Assigned Numbers." Service numbers for other applications are typically chosen from the range 1024 to 65535 by

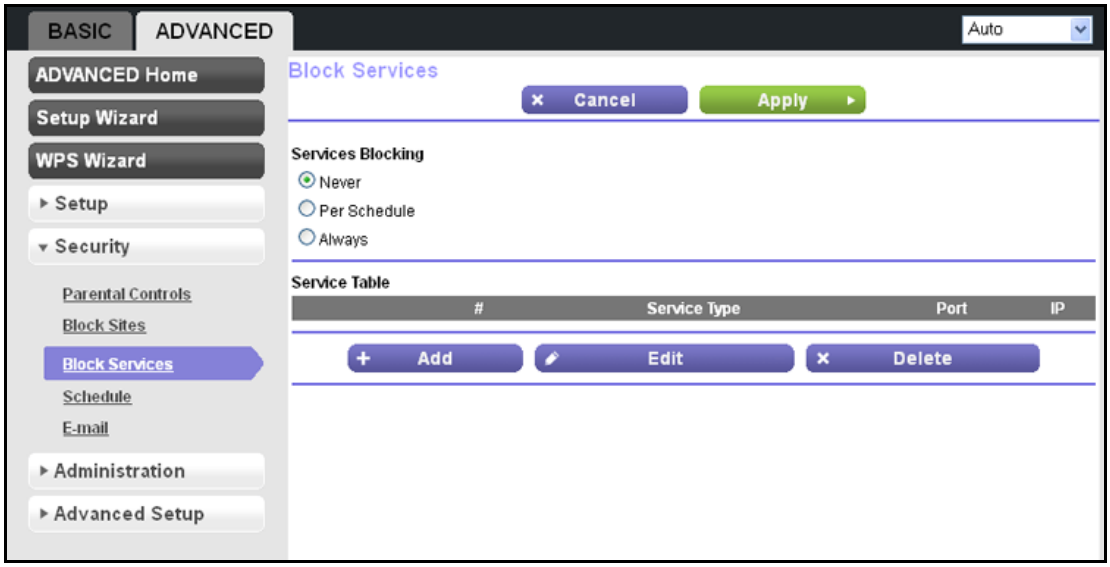
the authors of the application. Although the router already holds a list of many service port numbers, you are not limited to these choices. You can often determine port number information by contacting the publisher of the application, by asking user groups or newsgroups, or by searching.

The Block Services screen lets you add and block specific Internet services by computers on your network. This is called service blocking or port filtering. To add a service for blocking, first determine which port number or range of numbers is used by the application.

➢ **To block services:**

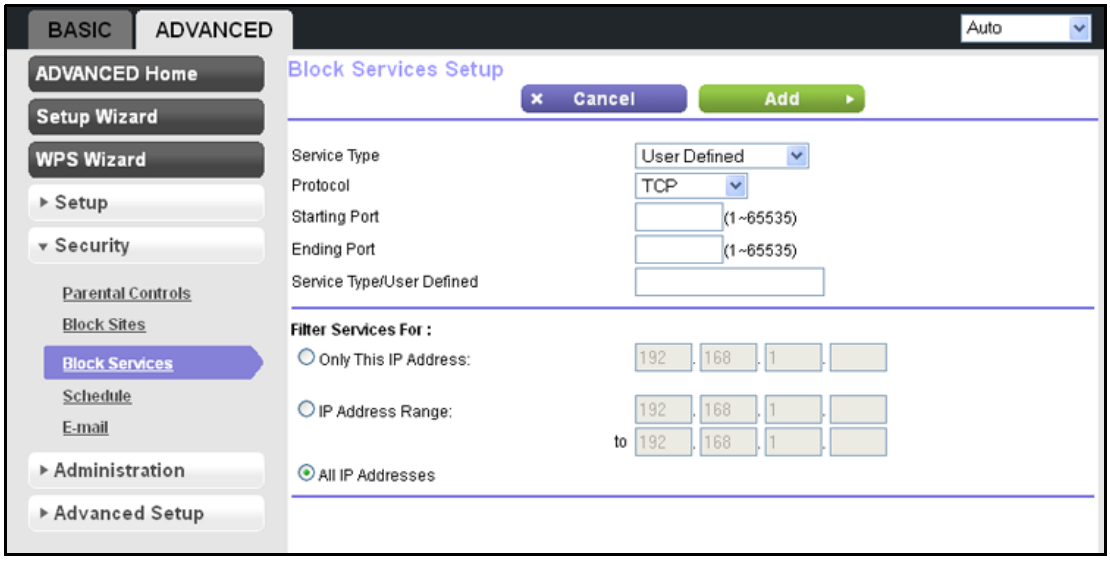
1. Select **Advanced > Security > Block Services**.

   The Block Services screen displays:



2. Select one of the service blocking options (by default, Never is selected):
   - **Per Schedule**. Turn on service blocking according to the settings on the Schedule screen (see *Schedule Blocking* on page 65).
   - **Always**. Turn on service blocking all the time, independent of the settings on the Schedule screen.
3. Click the **Add** button to add a service.

The Block Services Setup screen displays:



4. From the Service Type list, select the application or service to allow or block.

   The list already displays several common services, but you are not limited to these choices.

5. (Optional) To add any additional services or applications that do not already appear, select **User Defined**.
6. (Optional) If you selected User Defined in the previous step:
   a. If you know the protocol that the application uses, select **TCP** or **UDP**. If you are not sure, select **TCP/UDP**.
   b. Enter the starting and ending port numbers.

      If the application uses a single port number, enter that number in both fields.

   c. Type a descriptive name in the Service Type/User Defined field.
7. Select the radio button for the IP address configuration that you want to block, and enter the IP addresses.

   You can block the specified service for a single computer, a range of computers with consecutive IP addresses, or all computers on your network.

8. Click the **Add** button.

   The application or service is saved in the Service Table on the Block Services screen.

➢ **To edit or delete an application or service from the Service Table:**

1. Select **Advanced > Security > Block Services**.

   The Block Services screen displays.

2. In the Service Table, select the radio button next to the application or service that you want to edit or delete.

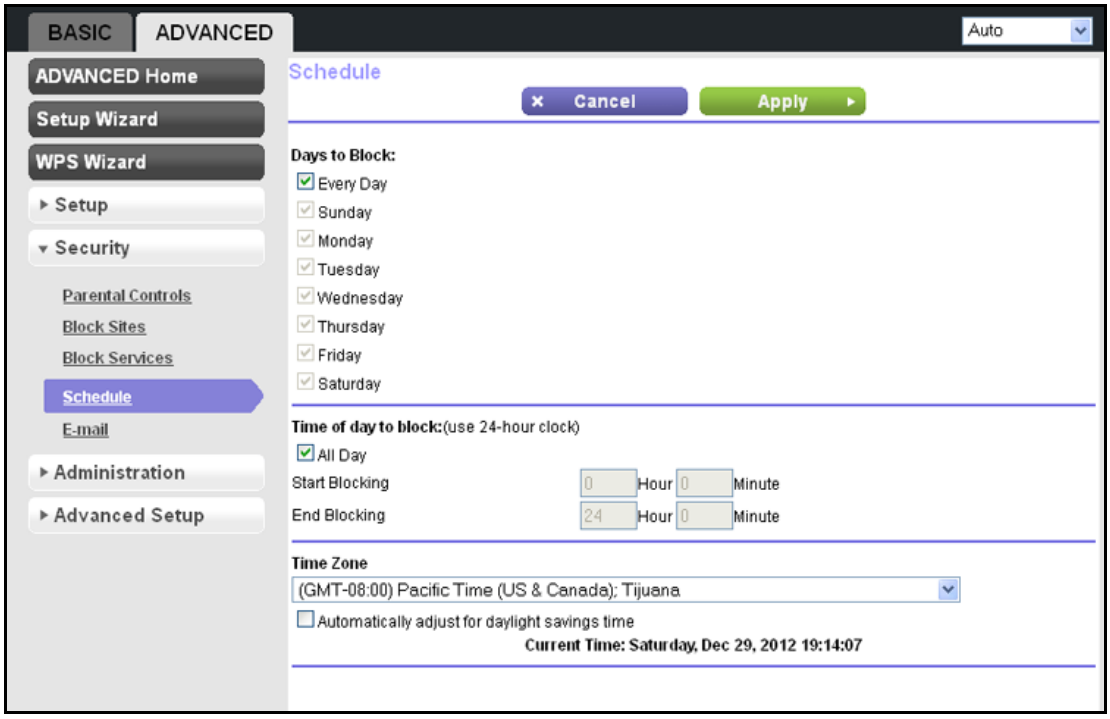
3. Do one of the following:
   - Click the **Edit** button to edit the application or service:
     a. Edit the application or service as described in the previous procedure.
     b. When you are done, click the **Accept** button.
   - Click the **Delete** button.
     The application or service is removed from the table.

Schedule Blocking

If you have set up keyword blocking, service blocking, or both, you can specify the days and time that you want blocking to occur.

➢ **To schedule blocking:**

1. Select **Advanced > Security > Schedule**.
   The Schedule screen displays:



2. Set up the schedule for blocking keywords and services:
   - **Days to Block**. Select days on which you want to apply blocking by selecting one or more individual check boxes, or select **Every Day** to select the check boxes for all days.
   - **Time of Day to Block**. Select a start and end time in 24-hour format, or select **All Day** for 24-hour blocking.
3. Select your time zone from the list.

4. If your time zone uses daylight saving time, select the **Automatically adjust for daylight savings time** check box.
5. Click the **Apply** button.

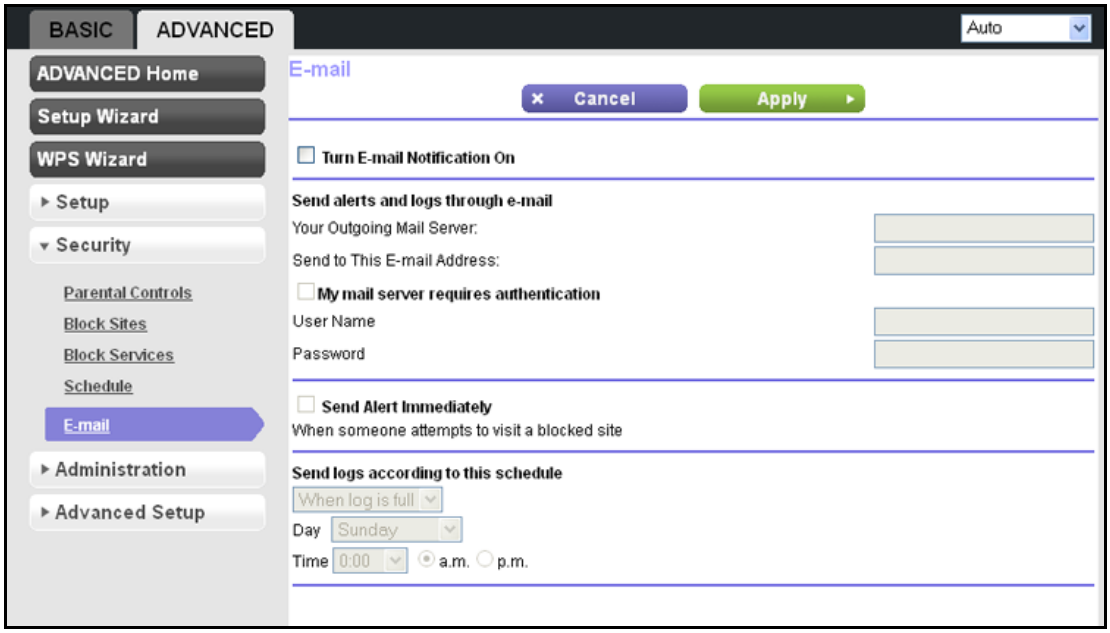
Security Event Email Notifications

To receive logs and alerts by email, provide your email information in the E-mail screen, and specify which alerts you want to receive and how often.

➢ **To set up email notifications:**

1. Select **Advanced > Security > E-mail**.

   The E-mail screen displays:



2. To receive email logs and alerts from the router, select the **Turn Email Notification On** check box.
3. In the Your Outgoing Mail Server field, enter the name of your ISP's outgoing (SMTP) mail server (such as mail.myISP.com).

   You might be able to find this information in the configuration screen of your email program. If you leave this field blank, log and alert messages are not sent by email.
4. Enter the email address to which logs and alerts are sent in the Send to This E-mail Address field.

   This email address is also used as the sender's email address. If you leave this field blank, log and alert messages are not sent by email.

5. If your outgoing email server requires authentication, select the **My Mail Server requires authentication** check box. Fill in the User Name and Password fields for the outgoing email server.
6. To have email alerts sent immediately when someone attempts to visit a blocked site or service, select **Send Alert Immediately**.
7. Specify when the logs are sent.

   If you select the Weekly, Daily, or Hourly option and the log fills up before the specified period, the log is automatically emailed to the specified email address. You can also select the log to be sent when the log is full.

   Note: *Whatever option you select, after the log is sent, the log is cleared from the router's memory. If the router cannot email the log file, the log buffer might fill up. In this case, the router overwrites the log and discards its contents.*

8. Click the **Apply** button.

Administration

6

Manage your network

This chapter describes the router settings for administering and maintaining your router and home network. This chapter includes the following sections:

- *Upgrade the Router Firmware*
- *View and Configure Logs*
- *Manage the Configuration File*

For information about changing the password of your router, see *Change the Password* on page 20.

For information about upgrading or checking the status of your router over the Internet, see *Remote Management* on page 100.

For information about monitoring the volume of Internet traffic passing through your router's Internet port, see *Traffic Meter* on page 112.

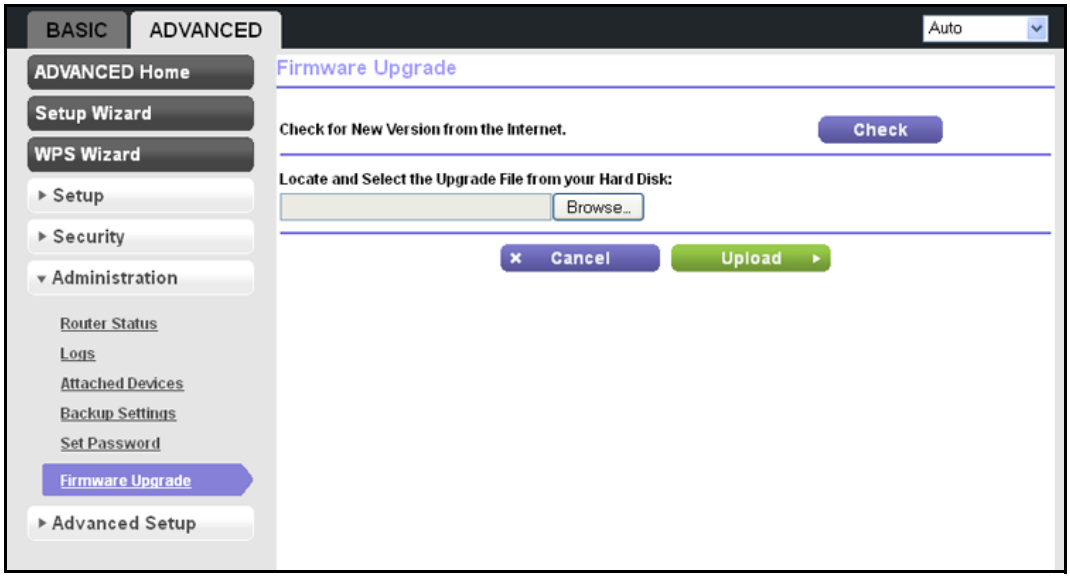
Upgrade the Router Firmware

The router's firmware (software) is stored in flash memory. If the router has detected that new firmware is available, you might see a message at the top of the genie screens. You can also use the Check button on the Firmware Upgrade screen to check manually if new firmware is available.

➢ **To check for new firmware and update your router:**

1. Select **Advanced > Administration > Firmware Upgrade**.

   The Firmware Upgrade screen displays:



2. Click the **Check** button.

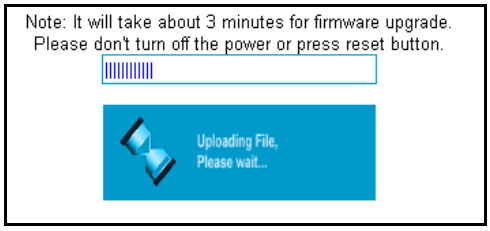
   The router detects new firmware if any is available. If new firmware is available, the Firmware Upgrade Assistant screen displays.

3. Click **Yes** to update the router to the new firmware.
4. (Optional) If you have manually downloaded new firmware from the NETGEAR support website:

   a. Click **Browse**, navigate to the firmware file (the file ends in .img), and select the firmware file.

   b. Click the **Upload** button.

   A progress bar shows the progress of the firmware upload process:



WARNING:

When uploading firmware to the router, *do not* interrupt the web browser by closing the window, clicking a link, or loading a new page. If the browser is interrupted, it could corrupt the firmware.

When the upload is complete, your router restarts. The upload process can take up to 3 minutes, and the upgrade process typically takes about 1 minute. Read the new firmware release notes to determine whether you need to reconfigure the router after upgrading.

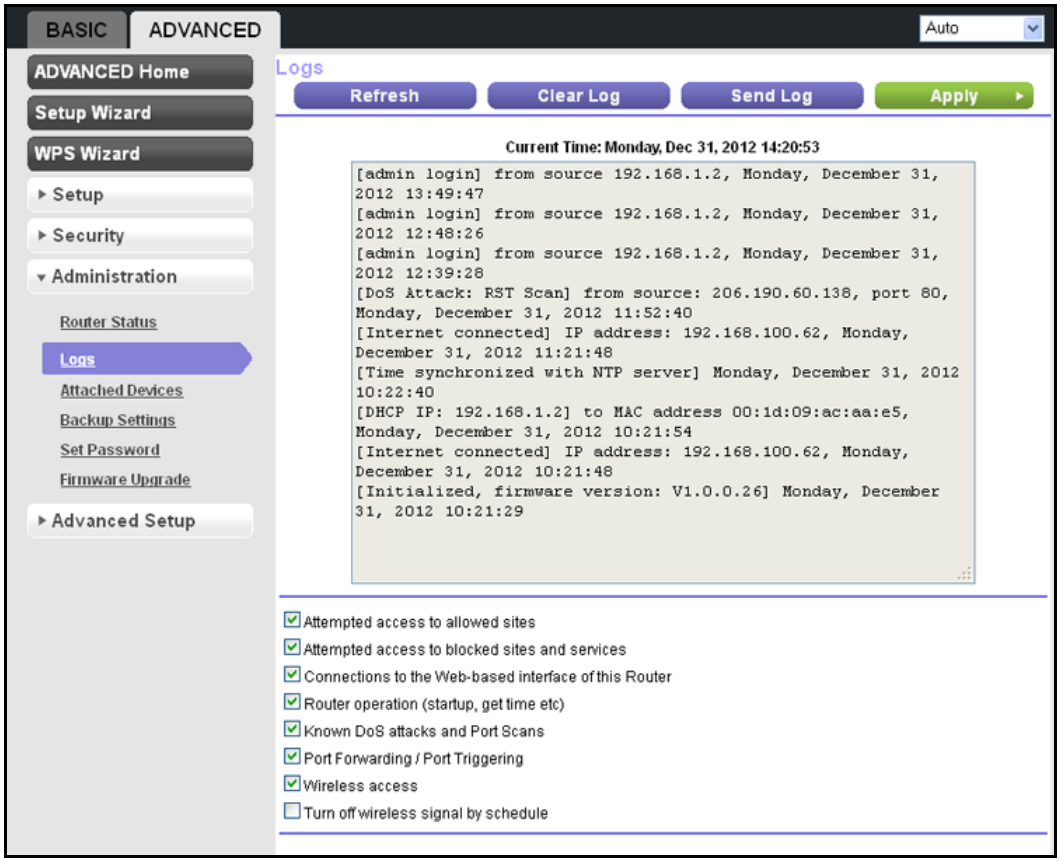
View and Configure Logs

The log is a detailed record of websites that users have accessed or attempted to access, router operation, DoS attacks and port scans, wireless access, and other information. Up to 256 entries are stored in the log.

➢ **To view the log:**

Select **Advanced > Administration > Logs**.

The Logs screen displays.



The Logs screen shows the following information:

Date and time. The date and time the log entry was recorded.

Source IP. The IP address of the initiating device for this log entry.

Target address. The name or IP address of the website or news group that users visited or attempted to access, or the IP address from which a DoS or port scan was initiated, from which time was synchronized, or in relation to which other actions occurred.

Action. The action that occurred.

To refresh the log screen, click the **Refresh** button.

To clear the log entries, click the **Clear Log** button.

To email the log immediately, click the **Send Log** button.

➢ **To configure which actions are logged:**

1. On the Logs screen, select any of the following check boxes:
   - **Attempted access to allowed sites**. Log attempts to access websites that are allowed.
   - **Attempted access to blocked sites and services**. Log attempts to access websites and services that are blocked.
   - **Connections to the Web-based interface of this Router**. Log access to the router user interface.
   - **Router operation (startup, get time etc)**. Log router operation events such as startup, Internet connection, firmware initialization, and time synchronization.
   - **Known DoS attacks and Port Scans**. Log DoS attacks and port scans.
   - **Port Forwarding / Port Triggering**. Log port forwarding and port triggering events.
   - **Wireless access**. Log access by wireless clients.
   - **Turn off wireless signal by schedule**. Log when the radio is turned off if the wireless signal is scheduled to be turned off.
2. Click the **Apply** button.

Manage the Configuration File

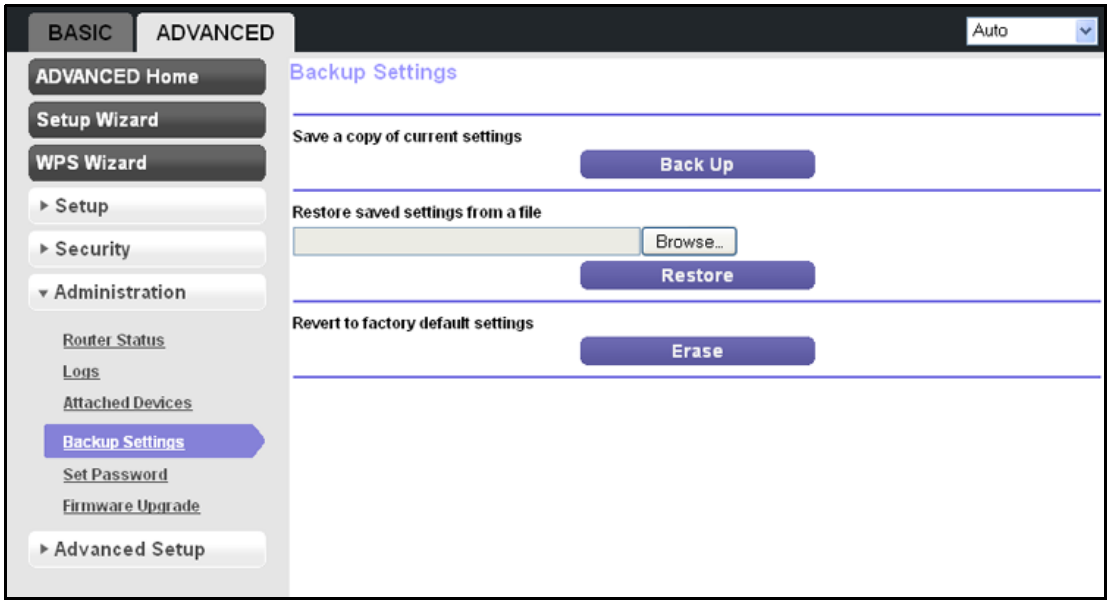
The configuration settings of the router are stored within the router in a configuration file. You can back up (save) this file to your computer, restore it, or reset it to the factory default settings.

Back Up Settings

➢ **To back up the router's configuration settings:**

1. Select **Advanced > Administration > Backup Settings**.

The Backup Settings screen displays:



2. Click the **Back Up** button to save a copy of the current settings.
3. Choose a location to store the .cfg file on a computer on your network.

Restore Configuration Settings

➢ **To restore configuration settings that you backed up:**

1. Select **Advanced > Administration > Backup Settings**.

   The Backup Settings screen displays.

2. Click the **Browse** button to navigate to the backup file (that is, the .cfg file).
3. Click the **Restore** button to upload the file to the router.

   Upon completion, the router reboots.

WARNING:

Do not interrupt the reboot process.

Erase

Under some circumstances (for example, if you move the router to a different network), you might want to erase the configuration and restore the factory default settings.

You can either use the Restore Factory Settings button on the back of the router (see *Factory Settings* on page 133), or you can use the Erase button on the Backup Settings screen.

➢ **To erase the configuration and restore the factory default settings:**

1. Select **Advanced > Administration > Backup Settings**.

   The Backup Settings screen displays.

2. Click the **Erase** button.
3. Click **Yes** to confirm the action.

The router reboots.

WARNING:

Do not interrupt the reboot process.

Erasing sets the user name to admin, the password to password, and the LAN IP address to 192.168.1.1, and enables the router's DHCP server.

Advanced Settings

7

This chapter describes the advanced features of your router. The information is for users with a solid understanding of networking concepts who want to set the router up for unique situations such as when remote access from the Internet by IP address or domain name is needed.

This chapter includes the following sections:

- *Advanced Wireless Settings*
- *Wireless Access Point (AP)*
- *Wireless Distribution System (WDS)*
- *Port Forwarding and Port Triggering Configuration Concepts*
- *Set Up Port Forwarding to Local Servers*
- *Set Up Port Triggering*
- *Dynamic DNS*
- *Static Routes*
- *Remote Management*
- *Universal Plug and Play*
- *IPv6*
- *Traffic Meter*

Advanced Wireless Settings

The Advanced Wireless Settings screen lets you configure advanced settings for your wireless network, set up a schedule to turn off your wireless network, configure the WPS settings, and set up an access list for wireless clients.

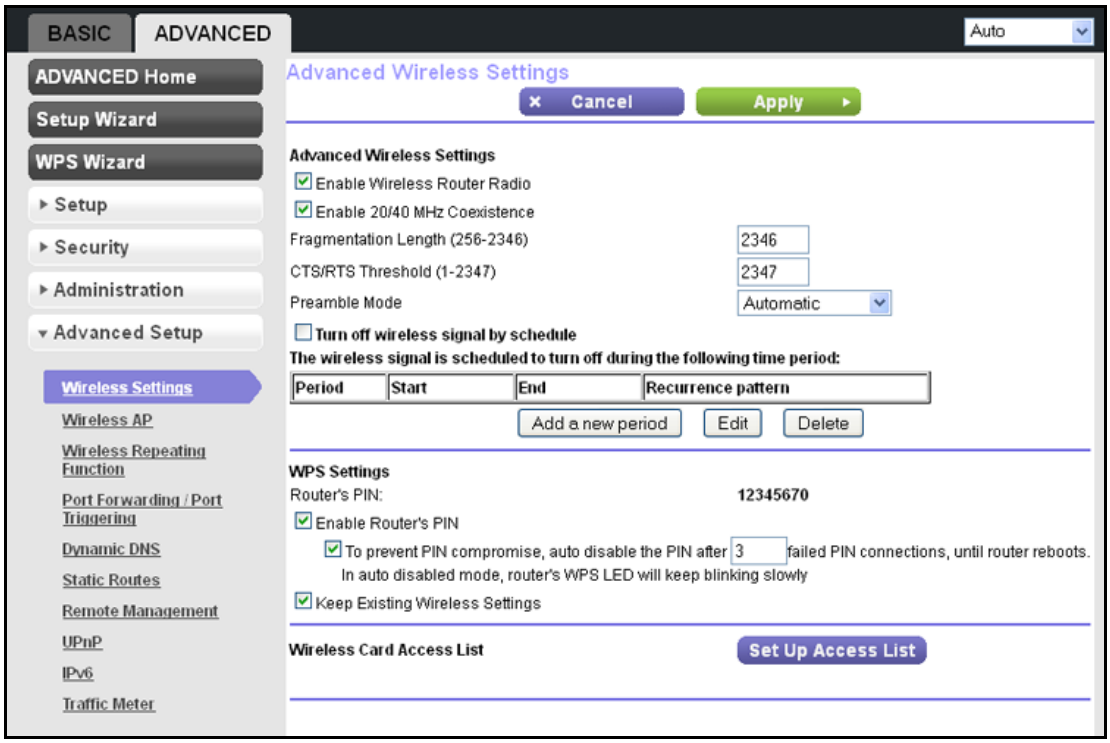
Advanced Settings for Your Wireless Network

NETGEAR recommends that you use caution changing these settings.

➢ **To change advanced settings for your wireless network:**

1. Select **Advanced > Advanced Setup > Wireless Settings**.

   The Advanced Wireless Settings screen displays:



2. (Optional) Clear the **Enable Wireless Router Radio** check box to completely turn off the wireless radio of the router.

   When the wireless radio is disabled, you can still use the router by connecting computers to the router with an Ethernet cable. By default, the wireless radio is enabled.

3. (Optional) Clear the **Enable 20/40 MHz Coexistence** check box to increase the wireless speed to the maximum supported speed.

   By default, 20/40 MHz coexistence is enabled to prevent interference between wireless network in your environment at the expense of the wireless speed. If there are no other

wireless networks in your environments, you can clear the Enable 20/40 MHz Coexistence check box.

IMPORTANT:

The Fragmentation Length, CTS/RTS Threshold, and Preamble Mode options are reserved for wireless testing and advanced configuration only. Do not change these settings.

4. Click the **Apply** button.

Set Up a Wireless Schedule

You can use this feature to turn off the wireless signal from your router at times when you do not need a wireless connection. For instance, you could turn it off for the weekend if you leave town.

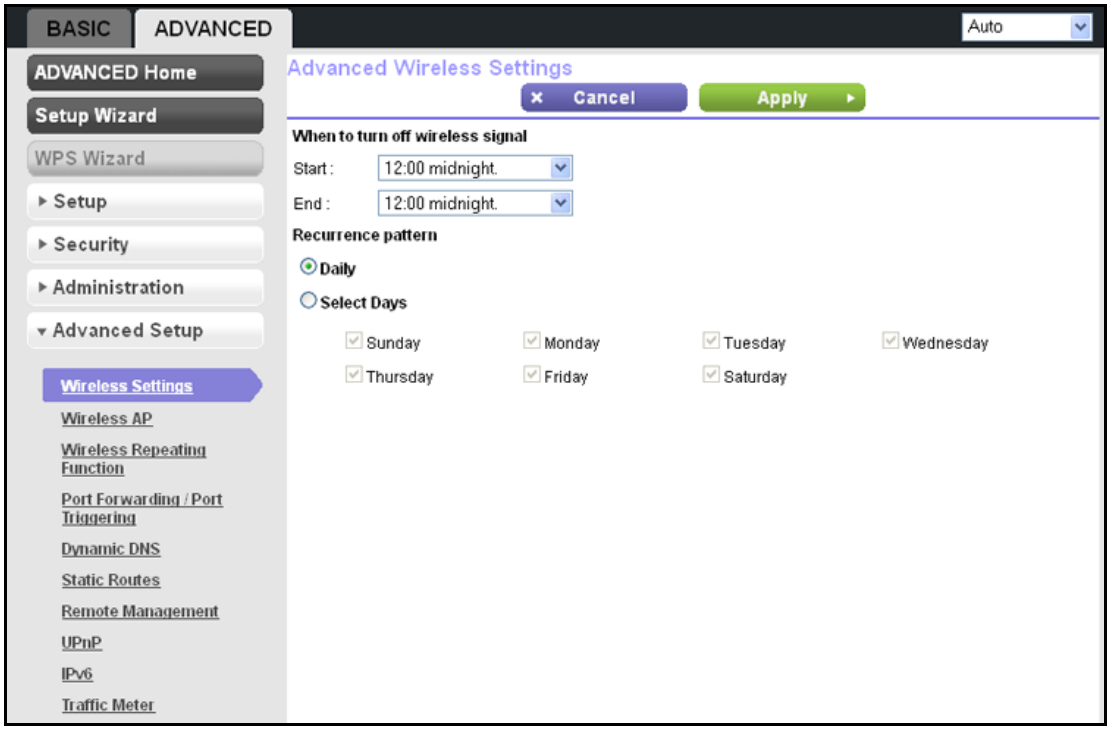
➢ **To configure and enable the wireless schedule:**

1. Select **Advanced > Advanced Setup > Wireless Settings**.

   The Advanced Wireless Settings screen displays.

2. Click the **Add a new period** button.

   The screen adjusts:



3. Use the menus, radio buttons, and check boxes to set up a period during which you want the wireless signal to be turned off.
4. Click the **Apply** button.

   The Advanced Wireless Settings screen displays.
5. Select the **Turn off wireless signal by schedule** check box to activate the schedule.
6. Click the **Apply** button.

Set Up the WPS Settings

You can control how WPS functions on the router. NETGEAR recommends that you use caution changing the WPS settings.

> **Note:** For information about how to use WPS to add wireless devices and other equipment to your wireless network, see *Wi-Fi Protected Setup (WPS) Method* on page 22.

You cannot set up the WPS settings when the security is WEP. Make sure that the security mode is WPA-PSK, WPA2-PSK, or WPA-PSK + WPA2-PSK Mixed Mode. For information about configuring the security mode, see *Basic Wireless Settings* on page 26.

You can do the following with the router's PIN:

- Disable the PIN entirely.
- Change the number of times that a PIN connection is allowed to fail before the PIN is automatically disabled. By default, the PIN is automatically disabled after three failed connection attempts. If the PIN is automatically disabled, it remains so until you restart the router. While the PIN is disabled, the WPS LED blinks slowly.
- Turn off automatic disabling of the PIN.

➢ **To change the WPS settings for your wireless network:**

1. Select **Advanced > Advanced Setup > Wireless Settings**.

   The Advanced Wireless Settings screen displays.

   The router's PIN is shown for information only. It cannot be changed.
2. (Optional) Clear the **Enable Router's PIN** check box to disable the router's PIN entirely.

   By default, the PIN is enabled, but there might be situations in which you want to disable the PIN.
3. (Optional) Under the Enable Router's PIN check box, type a number in the field to change the number of times that a PIN connection can fail.

   You can change this setting only when the PIN is enabled. By default, the number is 3.

4. (Optional) Clear the check box *under* the Enable Router's PIN check box to turn off automatic disabling of the PIN.

   You can change this setting only when the PIN is enabled. By default, automatic disabling of the PIN is turned on.

5. (Optional) Clear the **Keep Existing Wireless Settings** check box.

   By default, this check box is selected. However, when the check box is selected, some applications such as Network Explorer in Windows Vista might not detect the router.

   CAUTION: When you clear this check box and you add a new wireless client through WPS, the router's wireless settings change to an automatically generated SSID and passphrase (also referred to as the wireless network password or network key).

6. Click the **Apply** button.

Set Up a Wireless Card Access List

By default, any wireless device that is configured with the correct SSID is allowed access to your wireless network. For increased security, you can restrict access to the wireless network to allow only specific wireless devices based on their MAC addresses.

Note: If you use a wireless computer to set up a wireless card access list, add your wireless computer to the access list; otherwise, you are disconnected when you click the Apply button. To avoid this situation, use a computer with a wired connection to access the router.

➢ **To restrict access to your network to specific wireless devices:**

1. Select **Advanced > Advanced Setup > Wireless Settings**.

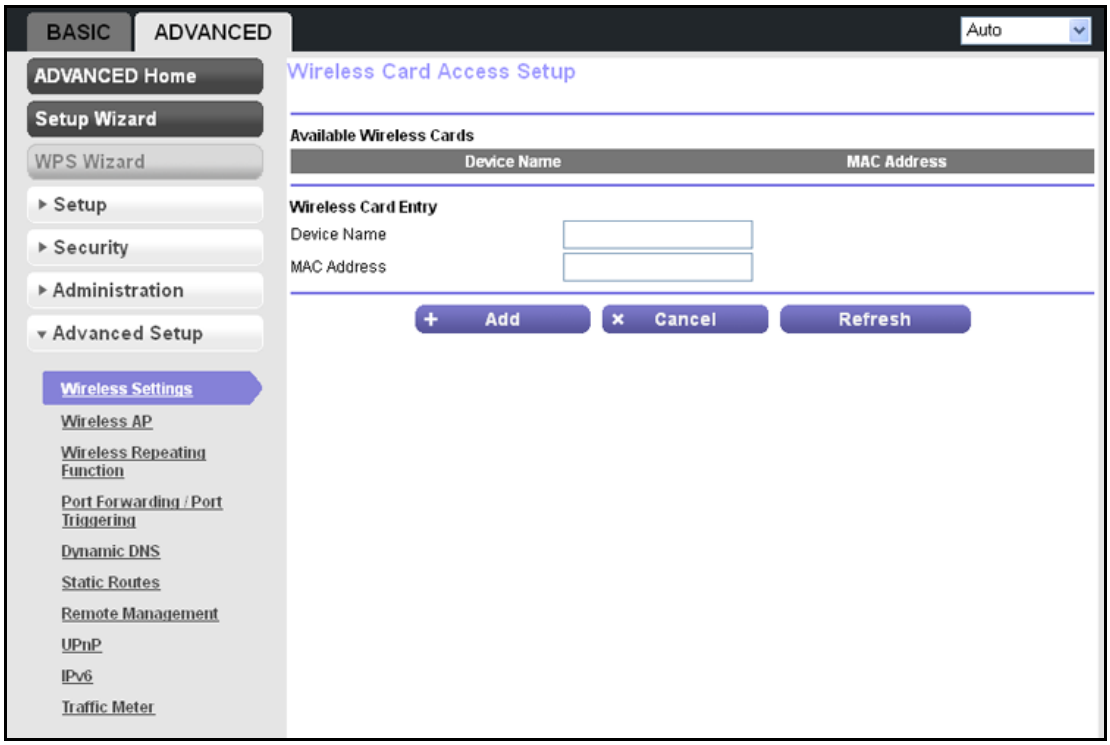
   The Advanced Wireless Settings screen displays.

2. Click the **Set Up Access List** button.

The Wireless Card Access List screen displays:

3. Click the **Add** button.

The Wireless Card Access Setup screen displays.



4. Type a name for the wireless device.
5. Type the MAC address of the wireless device.
6. Click the **Add** button to add the device to the table on the Wireless Card Access List screen.
7. (Optional) Repeat *Step 4* through *Step 6* for additional wireless devices.
8. Select the **Turn Access Control On** check box.
9. Click the **Apply** button.

   Now only wireless devices that are in the table on the Wireless Card Access List screen can access the router.

➢ **To edit or delete a wireless device from the access list:**

1. Select **Advanced > Advanced Setup > Wireless Settings**.

   The Advanced Wireless Settings screen displays.
2. In the table, select the radio button next to the wireless device that you want to edit or delete.
3. Do one of the following:
   - Click the **Edit** button.

     The Edit Wireless Card screen displays.

     a. Edit the address information.

     b. Click the **Accept** button.
   - Click the **Delete** button.

     The address is removed from the table.

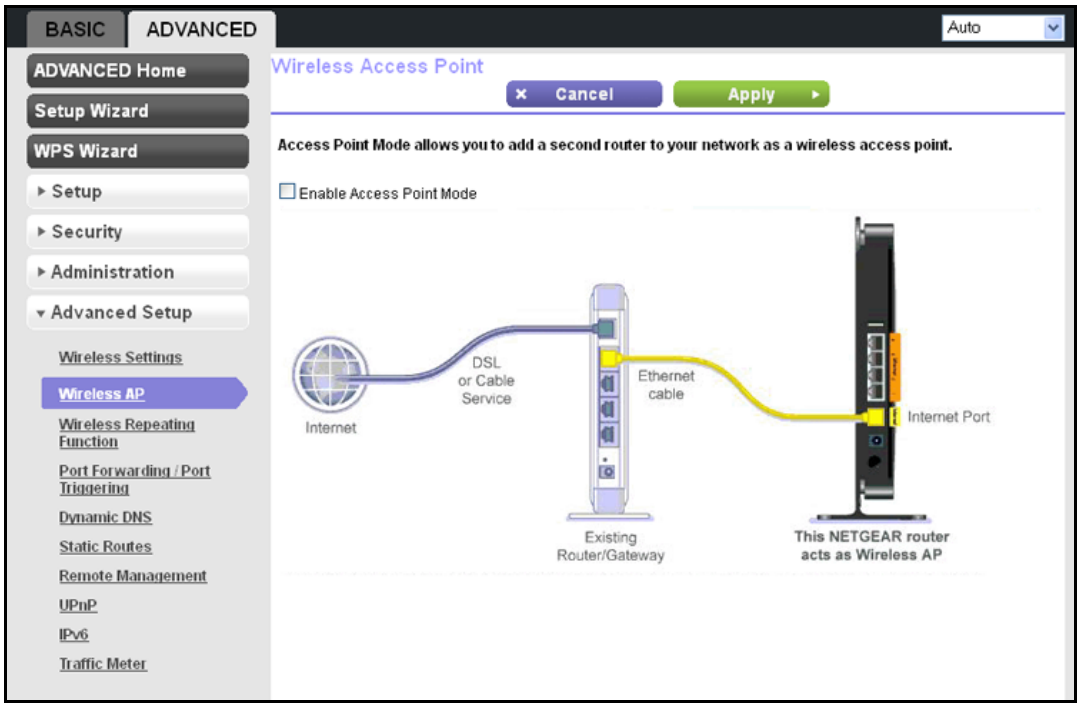
Wireless Access Point (AP)

The router can function in access point (AP) mode instead of regular router mode. In AP mode, the router can function as a bridge between wireless clients and another router or gateway in your network that connects to the Internet. When the router functions in AP mode, many router functions are disabled, but wireless clients can connect to the router, and you can still access the router to change the configuration, for example, to disable AP mode and return to regular router mode.

➢ **To enable and configure AP mode:**

1. Select **Advanced > Advanced Setup > Wireless AP**.

The Wireless Access Point screen displays:



2. Select the **Enable Access Point Mode** check box.

   The screen adjusts.

3. Configure the IP address settings for the router:
   - **Get dynamically from existing router**. By default, the Get dynamically from existing router radio button is selected, enabling the router to receive its IP address and other IP settings from the other router or gateway in your network.
   - **Use fixed IP Address**. Select the Use fixed IP Address radio button to set up static IP address settings.

     NETGEAR does not recommend this setting.

Note: If the other router or gateway in your network also has wireless capability, NETGEAR recommends that you use wireless settings on your router that are different from those on the other router or gateway to avoid interference. You could also disable the wireless radio on the other router or gateway and use your router only for wireless client access.

4. Click the **Apply** button.

Note: When you click the **Apply** button, the IP address of the router changes and you are disconnected. To reconnect, close and restart your web browser, and type **http://www.routerlogin.net**.

Wireless Distribution System (WDS)

You can set up the router to be used as a wireless base station or wireless repeater in a wireless distribution system (WDS). A WDS lets you expand a wireless network through multiple access points instead of using a wired backbone to link them. A wireless base station connects to the Internet, can have wired and wireless clients, and sends its wireless signal to an access point that functions as a wireless repeater. A wireless repeater can also have wired and wireless clients, but connects to the Internet through the wireless base station.

The following figure shows a wireless repeating scenario.

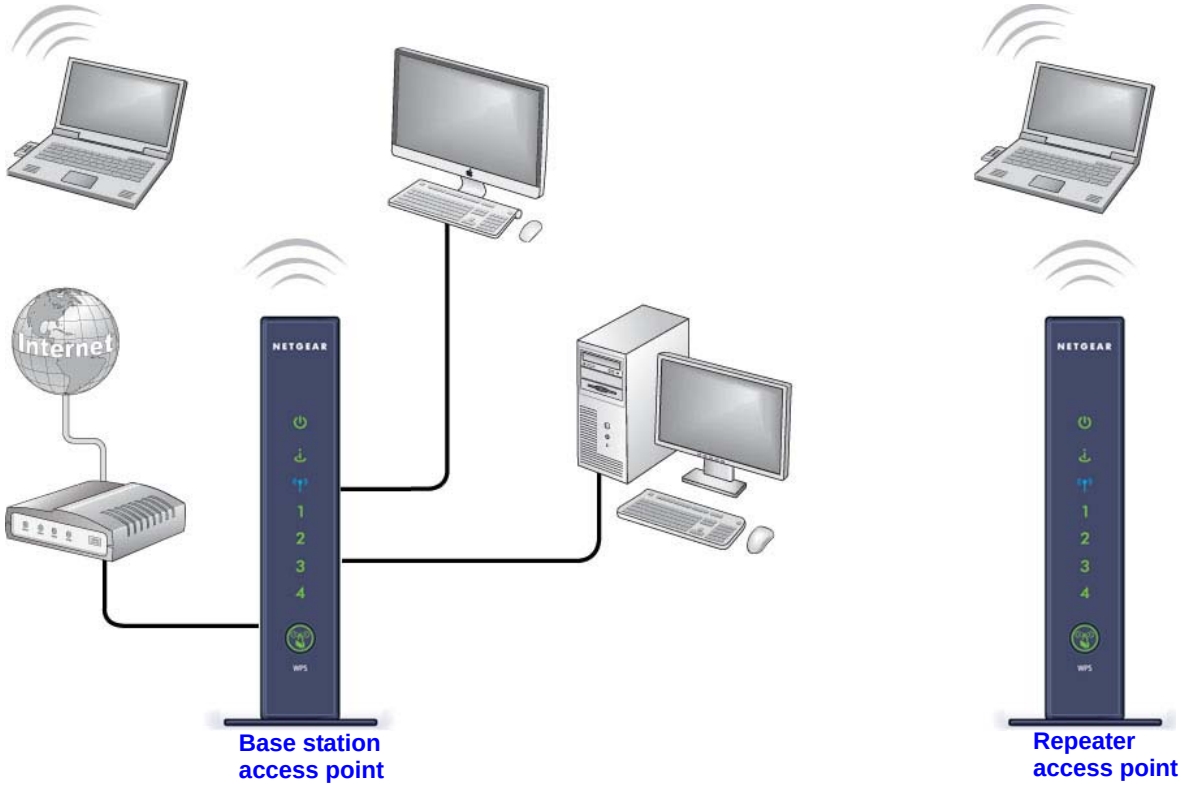


Figure 10. Wireless repeating scenario

The router can function either as a base station or as a repeater:

- **Wireless base station**. The router acts as the parent access point, bridging traffic to and from the child repeater access point, as well as handling wireless and wired local computers. To configure this mode, you need to know the MAC addresses of the child repeater access point.
- **Wireless repeater**. The router sends all traffic from its local wireless or wired computers to a remote access point. To configure this mode, you need to know the MAC address of the remote parent access point.

For you to set up a wireless network in a WDS, the following conditions need to be met for both access points:

- Both access points need to use the same SSID, wireless channel, and encryption mode.
- Both access points need to be on the same LAN IP subnet. That is, all the access point LAN IP addresses are in the same network.
- All LAN devices (wired and wireless computers) need to be configured to operate in the same LAN network address range as the access points.
- The channel selection on the access points cannot be Auto (see *Basic Wireless Settings* on page 26).
- The security option needs to be WEP (or no security). The WEP option displays only if you select Up to 54 Mbps from the Mode menu on the Wireless Settings screen (see *Basic Wireless Settings* on page 26).

Set Up the Base Station

The wireless repeating function works only in hub and spoke mode. The units cannot be daisy-chained. You need to know the wireless MAC addresses of all units. First, set up the base station, and then set up the repeater.

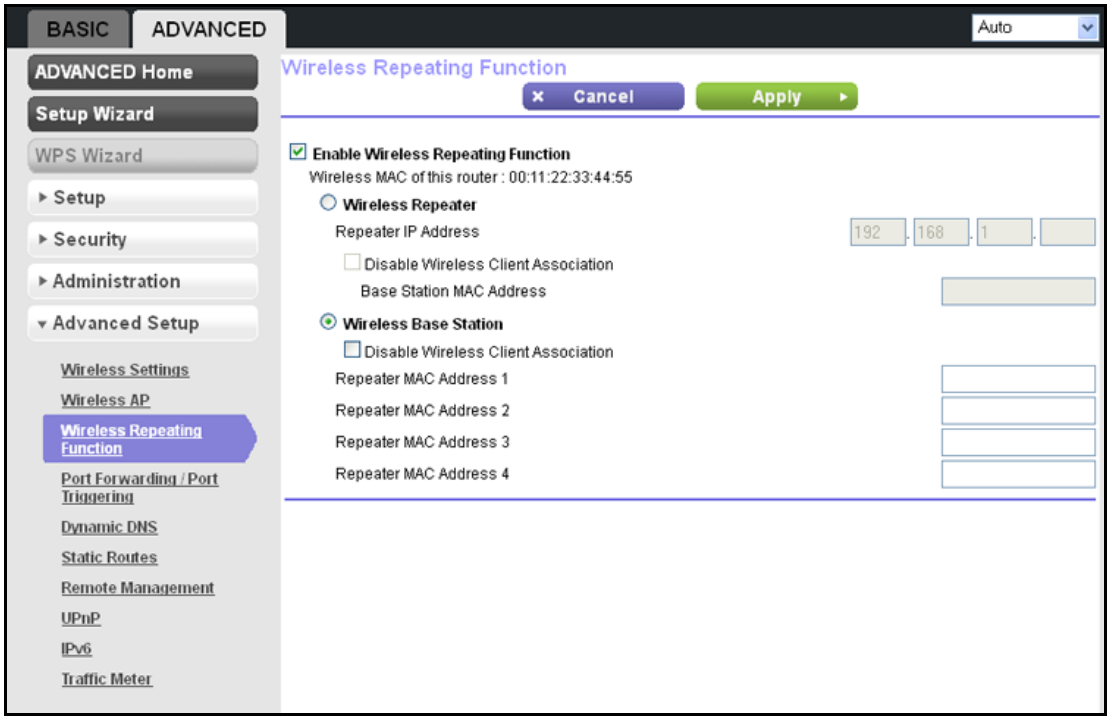
➢ **To set up the base station:**

1. Select **Advanced > Advanced Setup > Wireless Repeating Function**.

   The Wireless Repeating Function screen displays. The wireless MAC address of the router is displayed onscreen.

2. Select the **Enable Wireless Repeating Function** check box.

3. Select the **Wireless Base Station** radio button.



4. (Optional) Select the **Disable Wireless Client Association** check box to prevent wireless clients from associating with the base station and allowing LAN client associations only. You can leave the check box cleared if you prefer wireless clients to be able to associate with the base stations.
5. In the Repeater MAC Address 1 through 4 fields, enter the MAC addresses for the access points that should function as repeaters.

   If your router is the base station, it can function as the “parent” for up to 4 other access points.
6. Click the **Apply** button.

Set Up a Repeater

Use a wired Ethernet connection to set up the repeater to avoid conflicts with the wireless connection to the base station.

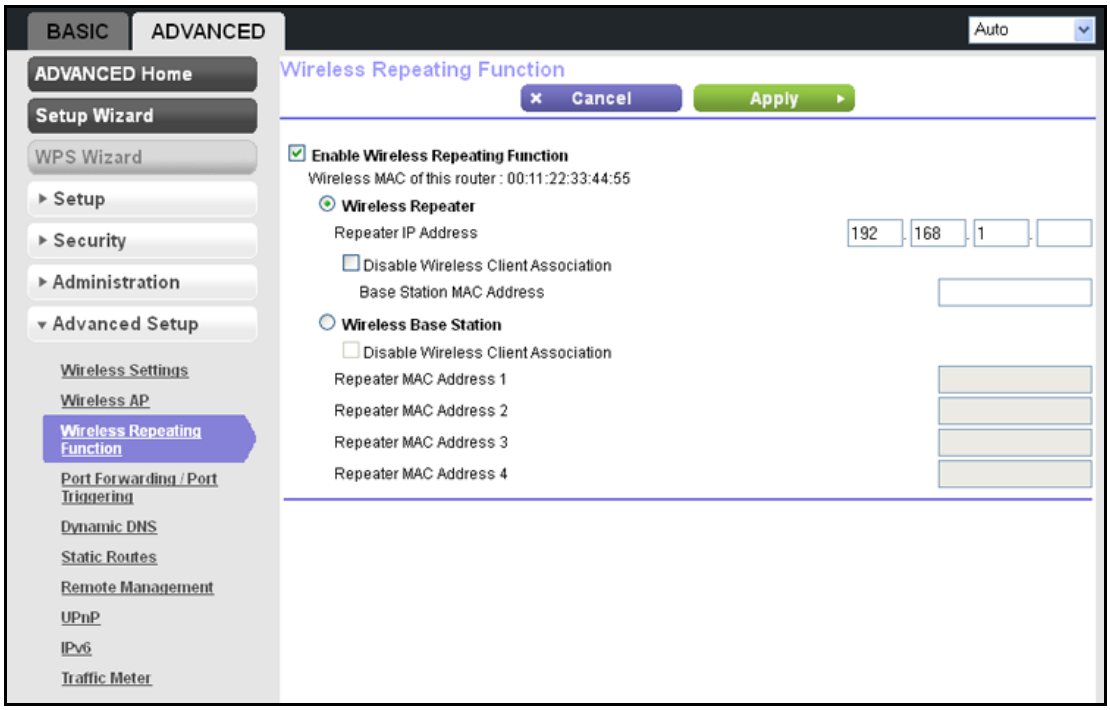
Note: If you set up the your router as a base station with a non-NETGEAR access point as the repeater, you might need to change additional configuration settings. In particular, you should disable the DHCP server function on the access point that functions as the repeater.

➢ **To configure the router as a repeater:**

1. Select **Advanced > Advanced Setup > Wireless Repeating Function**.

   The Wireless Repeating Function screen displays. The wireless MAC address of the router is displayed onscreen.

2. Select the **Enable Wireless Repeating Function** check box.
3. Select the **Wireless Repeater** radio button.



4. Fill in the Repeater IP Address field.

   This IP address has to be in the same subnet as the base station, but different from the LAN IP address of the base station.

5. (Optional) Select the **Disable Wireless Client Association** check box to prevent wireless clients from associating with the repeater and allowing LAN client associations only.

   You can leave the check box cleared if you prefer wireless clients to be able to associate with the repeater.

6. In the Base Station MAC Address field, enter the MAC addresses for the access point that should function as the base station.
7. Click the **Apply** button.
8. Verify connectivity across the LANs.

   A computer on any wireless or wired LAN segment of the base station or a repeater should be able to connect to the Internet. Any computer that is connected to the base station should be able to share files and printers with any other wireless or wired computer or server that is connected to a repeater, and the other way around.

Port Forwarding and Port Triggering Configuration Concepts

By default, the router blocks inbound traffic from the Internet to your computers except replies to your outbound traffic. You might need to create exceptions to this rule for these purposes:

- To allow remote computers on the Internet to access a server on your local network.
- To allow certain applications and games to work correctly when their replies are not recognized by your router.

Your router provides two features for creating these exceptions: port forwarding and port triggering. The next sections provide background information to help you understand how port forwarding and port triggering work, and the differences between the two.

Remote Computer Access Basics

When a computer on your network needs to access a computer on the Internet, your computer sends your router a message containing the source and destination address and process information. Before forwarding your message to the remote computer, your router has to modify the source information and create and track the communication session so that replies can be routed back to your computer.

Here is an example of normal outbound traffic and the resulting inbound responses:

1. You open a browser, and your operating system assigns port number 5678 to this browser session.
2. You type http://www.example.com into the URL field, and your computer creates a web page request message with the following address and port information. The request message is sent to your router.
   - **Source address**. Your computer's IP address.
   - **Source port number**. 5678, which is the browser session.
   - **Destination address**. The IP address of www.example.com, which your computer finds by asking a DNS server.
   - **Destination port number**. 80, which is the standard port number for a web server process.
3. Your router creates an entry in its internal session table describing this communication session between your computer and the web server at www.example.com. Before sending the web page request message to www.example.com, your router stores the original information and then modifies the source information in the request message, performing Network Address Translation (NAT):
   - The source address is replaced with your router's public IP address. This is necessary because your computer uses a private IP address that is not globally unique and cannot be used on the Internet.
   - The source port number is changed to a number chosen by the router, such as 33333. This is necessary because two computers could independently be using the same session number.

Your router then sends this request message through the Internet to the web server at www.example.com.

4. The web server at www.example.com composes a return message with the requested web page data. The return message contains the following address and port information. The web server then sends this reply message to your router.
   - **Source address**. The IP address of www.example.com.
   - **Source port number**. 80, which is the standard port number for a web server process.
   - **Destination address**. The public IP address of your router.
   - **Destination port number**. 33333.
5. Upon receiving the incoming message, your router checks its session table to determine whether there is an active session for port number 33333. Finding an active session, the router then modifies the message to restore the original address information replaced by NAT. Your router sends this reply message to your computer, which displays the web page from www.example.com. The message now contains the following address and port information.
   - **Source address**. The IP address of www.example.com.
   - **Source port number**. 80, which is the standard port number for a web server process.
   - **Destination address**. Your computer's IP address.
   - **Destination port number**. 5678, which is the browser session that made the initial request.
6. When you finish your browser session, your router eventually detects a period of inactivity in the communications. Your router then removes the session information from its session table, and incoming traffic is no longer accepted on port number 33333.

Port Triggering to Open Incoming Ports

In the preceding example, requests are sent to a remote computer by your router from a particular service port number, and replies from the remote computer to your router are directed to that port number. If the remote server sends a reply back to a different port number, your router does not recognize it and discards it. However, some application servers (such as FTP and IRC servers) send replies back to multiple port numbers. Using the port triggering function of your router, you can tell the router to open additional incoming ports when a particular outgoing port originates a session.

An example is Internet Relay Chat (IRC). Your computer connects to an IRC server at destination port 6667. The IRC server not only responds to your originating source port, but also sends an "identify" message to your computer on port 113. Using port triggering, you can tell the router, "When you initiate a session with destination port 6667, you have to also allow incoming traffic on port 113 to reach the originating computer."

Using steps similar to the preceding example, the following sequence shows the effects of the port triggering rule you have defined:

1. You open an IRC client program to start a chat session on your computer.
2. Your IRC client composes a request message to an IRC server using a destination port number of 6667, the standard port number for an IRC server process. Your computer then sends this request message to your router.
3. Your router creates an entry in its internal session table describing this communication session between your computer and the IRC server. Your router stores the original information, performs Network Address Translation (NAT) on the source address and port, and sends this request message through the Internet to the IRC server.
4. Noting your port triggering rule and having observed the destination port number of 6667, your router creates an additional session entry to send any incoming port 113 traffic to your computer.
5. The IRC server sends a return message to your router using the NAT-assigned source port (as in the previous example, say port 33333) as the destination port. The IRC server also sends an “identify” message to your router with destination port 113.
6. Upon receiving the incoming message to destination port 33333, your router checks its session table to determine whether there is an active session for port number 33333. Finding an active session, the router restores the original address information replaced by NAT and sends this reply message to your computer.
7. Upon receiving the incoming message to destination port 113, your router checks its session table and learns that there is an active session for port 113 associated with your computer. The router replaces the message’s destination IP address with your computer’s IP address and forwards the message to your computer.
8. When you finish your chat session, your router eventually senses a period of inactivity in the communications. The router then removes the session information from its session table, and incoming traffic is no longer accepted on port numbers 33333 or 113.

To configure port triggering, you need to know which inbound ports the application needs. Also, you need to know the number of the outbound port that triggers the opening of the inbound ports. You can usually determine this information by contacting the publisher of the application or user groups or newsgroups.

Note: Only one computer at a time can use the triggered application.

Port Forwarding to Permit External Host Communications

In both of the preceding examples, your computer initiates an application session with a server computer on the Internet. However, you might need to allow a client computer on the Internet to initiate a connection to a server computer on your network. Normally, your router ignores any inbound traffic that is not a response to your own outbound traffic. You can configure exceptions to this default rule by using the port forwarding feature.

A typical application of port forwarding can be shown by reversing the client-server relationship from the previous web server example. In this case, a remote computer’s

browser needs to access a web server running on a computer in your local network. Using port forwarding, you can tell the router, “When you receive incoming traffic on port 80 (the standard port number for a web server process), forward it to the local computer at 192.168.1.123.” The following sequence shows the effects of the port forwarding rule you have defined:

1. The user of a remote computer opens a browser and requests a web page from www.example.com, which resolves to the public IP address of your router. The remote computer composes a web page request message with the following destination information:

   Destination address. The IP address of www.example.com, which is the address of your router.

   Destination port number. 80, which is the standard port number for a web server process.

   The remote computer then sends this request message through the Internet to your router.

2. Your router receives the request message and looks in its rules table for any rules covering the disposition of incoming port 80 traffic. Your port forwarding rule specifies that incoming port 80 traffic should be forwarded to local IP address 192.168.1.123. Therefore, your router modifies the destination information in the request message:

   The destination address is replaced with 192.168.1.123.

   Your router then sends this request message to your local network.

3. Your web server at 192.168.1.123 receives the request and composes a return message with the requested web page data. Your web server then sends this reply message to your router.
4. Your router performs Network Address Translation (NAT) on the source IP address and sends this request message through the Internet to the remote computer, which displays the web page from www.example.com.

To configure port forwarding, you need to know which inbound ports the application needs. You usually can determine this information by contacting the publisher of the application or the relevant user groups and newsgroups.

How Port Forwarding Differs from Port Triggering

The following points summarize the differences between port forwarding and port triggering:

- Port triggering can be used by any computer on your network, although only one computer can use it at a time.
- Port forwarding is configured for a single computer on your network.
- Port triggering does not require that you know the computer’s IP address in advance. The IP address is captured automatically.
- Port forwarding requires that you specify the computer’s IP address during configuration, and the IP address can never change.

- Port triggering requires specific outbound traffic to open the inbound ports, and the triggered ports are closed after a period of no activity.
- Port forwarding is always active and does not need to be triggered.

Set Up Port Forwarding to Local Servers

Using the port forwarding feature, you can allow certain types of incoming traffic to reach servers on your local network. For example, you might want to make a local web server, FTP server, or game server visible and available to the Internet.

Use the Port Forwarding screen to configure the router to forward specific incoming protocols to computers on your local network. In addition to servers for specific applications, you can also specify a default DMZ server to which all other incoming protocols are forwarded.

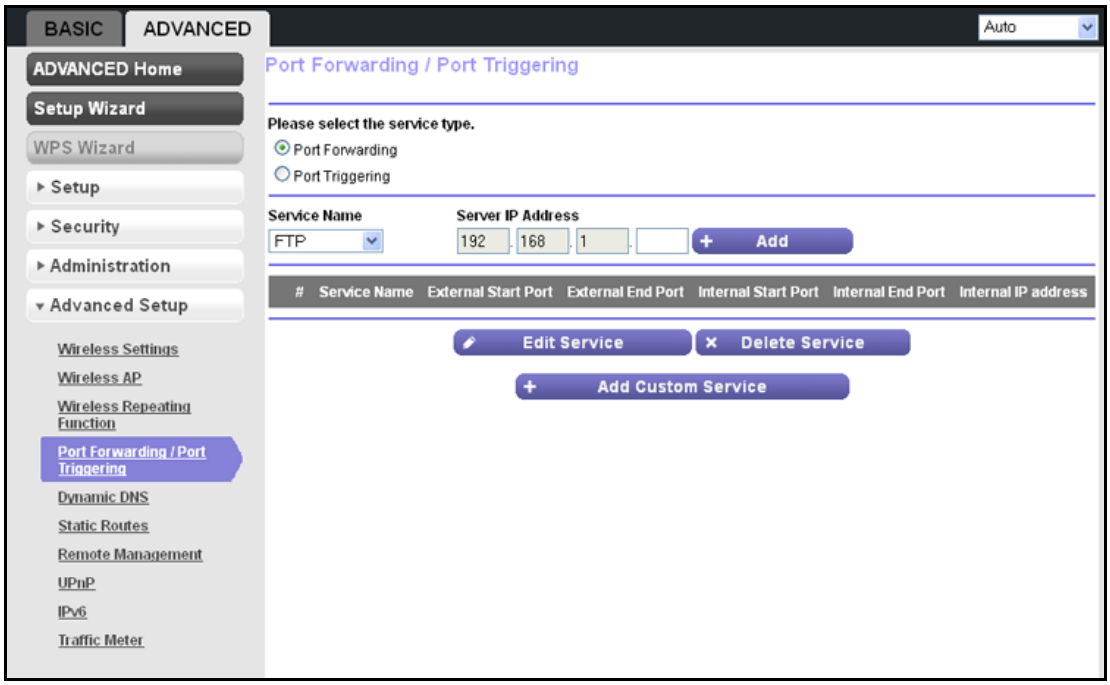
Before starting, you need to determine which type of service, application, or game you want to provide, and the local IP address of the computer that should provide the service. The server computer has to always have the same IP address.

Tip: To ensure that your server computer always has the same IP address, use the reserved IP address feature (see *Set Up Address Reservation* on page 49) of your router.

➢ **To set up port forwarding:**

1. Select **Advanced Setup > Port Forwarding / Port Triggering**.

   The Port Forwarding / Port Triggering screen displays.



By default, Port Forwarding is selected as the service type.

2. From the Service Name list, select the service or game that you are hosting on your network.

   If the service does not appear in the list, see *Add a Custom Service* on page 91.

3. In the corresponding Server IP Address field, enter the last octet of the IP address of your local computer that provides this service.
4. Click the **Add** button.

   The service is added to the table onscreen.

Add a Custom Service

To define a service, game, or application that does not appear in the Service Name list, you have to first determine which port number or range of numbers is used by the application. You can usually determine this information by contacting the publisher of the application or user groups or newsgroups.

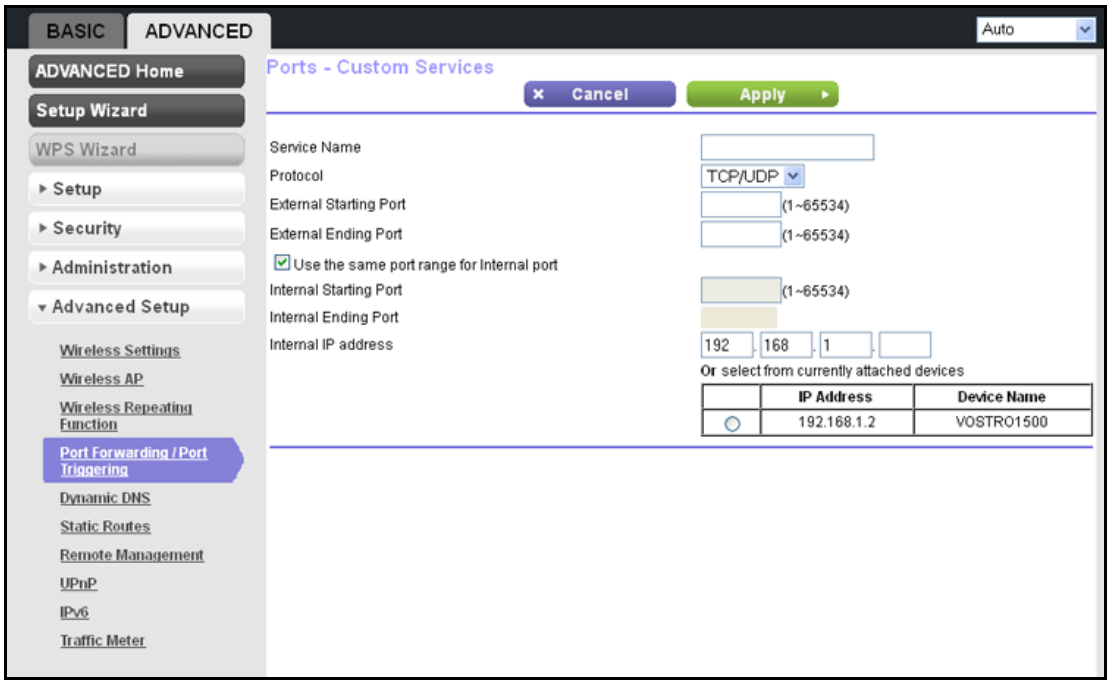
➢ **To add a custom service:**

1. Select **Advanced Setup > Port Forwarding / Port Triggering**.

   The Port Forwarding / Port Triggering screen displays. By default, Port Forwarding is selected as the service type.

2. Click the **Add Custom Service** button.

   The Ports - Custom Services screen displays:



3. In the Service Name field, enter a descriptive name.

4. In the Protocol list, select the protocol. Select **TCP**, **UDP**, or **TCP/UDP**. If you are not sure, select **TCP/UDP**.
5. In the External Starting Port field, enter the beginning port number.
   - If the application uses a single port, enter the same port number in the External Ending Port field.
   - If the application uses a range of ports, enter the ending port number of the range in the External Ending Port field.
6. If the internal port numbers are the same as the external port numbers, select the **Use the same port range for Internal port** check box. If they are not, use the Internal Starting Port and Internal Ending Port fields to enter the port numbers.
7. In the Internal IP Address field, enter the IP address of your local computer that provides this service.

   You can also select a radio button for one of the devices in the list of attached devices to automatically place the IP address of the selected device in the Internal IP Address field.
8. Click the **Apply** button.

   The service is added to the table on the Port Forwarding / Port Triggering screen.

Edit or Delete a Port Forwarding Entry

➢ **To edit or delete a port forwarding entry:**

1. Select **Advanced > Advanced Setup > Port Forwarding / Port Triggering**.

   The Port Forwarding / Port Triggering screen displays.
2. In the table, select the radio button next to the service that you want to edit or delete.
3. Do one of the following:
   - Click the **Edit Service** button.

     The Ports - Custom Services screen displays.

     a. Edit the service.

     b. Click the **Apply** button.
   - Click the **Delete Service** button.

     The service is removed from the table.

Application Example: Make a Local Web Server Public

If you host a web server on your local network, you can use port forwarding to allow web requests from anyone on the Internet to reach your web server.

➢ **To make a local web server public:**

1. Assign your web server either a fixed IP address or a dynamic IP address using DHCP address reservation.

   In this example, your router always gives your web server an IP address of 192.168.1.33.

2. On the Port Forwarding screen, configure the router to forward the HTTP service to the local address of your web server at 192.168.1.33.

   HTTP (port 80) is the standard protocol for web servers.

3. (Optional) Register a host name with a Dynamic DNS service, and configure your router to use the name.

   For more information, see *Dynamic DNS* on page 96. To access your web server from the Internet, a remote user has to know the IP address that has been assigned by your ISP. However, if you use a Dynamic DNS service, the remote user can reach your server by a user-friendly Internet name, such as mynetgear.dyndns.org.

Set Up Port Triggering

Port triggering is a dynamic extension of port forwarding that is useful in these cases:

- More than one local computer needs port forwarding for the same application (but not simultaneously).
- An application needs to open incoming ports that are different from the outgoing port.

When port triggering is enabled, the router monitors outbound traffic looking for a specified outbound trigger port. When the router detects outbound traffic on that port, it remembers the IP address of the local computer that sent the data. The router then temporarily opens the specified incoming port or ports, and forwards incoming traffic on the triggered ports to the triggering computer.

While port forwarding creates a static mapping of a port number or range to a single local computer, port triggering can dynamically open ports to any computer that needs them and can close the ports when they are no longer needed.

Note: If you use applications such as multiplayer gaming, peer-to-peer connections, real-time communications such as instant messaging, or remote assistance, you should also enable Universal Plug and Play (UPnP) according to the instructions in *Universal Plug and Play* on page 101.

To set up port triggering, you need to know which inbound ports the application needs. Also, you need to know the number of the outbound port that triggers the opening of the inbound ports. You can usually determine this information by contacting the publisher of the application or user groups or newsgroups.

➢ **To set up port triggering:**

1. Select **Advanced > Advanced Setup > Port Forwarding / Port Triggering**.

   The Port Forwarding / Port Triggering screen displays.

2. Select the **Port Triggering** radio button.

   The screen adjusts to display the port triggering information:

3. Clear the **Disable Port Triggering** check box if it is selected.

   Note: *If the Disable Port Triggering check box is selected after you configure port triggering, port triggering is disabled. However, any port triggering configuration information you added to the router is retained even though it is not used.*

4. In the Port Triggering Time-out field, enter a value up to 9999 minutes.

   The default value is 20 minutes. This value controls the inactivity timer for the designated inbound ports. The inbound ports close when the inactivity time expires because the router cannot detect when the application has terminated.

5. Click the **Add Service** button.

The Port Triggering - Services screen displays:

6. In the Service Name field, type a descriptive service name.
7. In the Service User list, select **Any** (the default) to allow this service to be used by any computer on the Internet. Otherwise, select **Single address**, and enter the IP address of one computer to restrict the service to a particular computer.
8. In the Service Type list, select the protocol. Select either **TCP** or **UDP**.
9. In the Triggering Port field, enter the number of the outbound traffic port that should cause the inbound ports to be opened.
10. Enter the inbound connection port information in the Connection Type, Starting Port, and Ending Port fields.
11. Click the **Apply** button.

    The service is added to the Port Triggering Portmap table on the Port Forwarding / Port Triggering screen. By default, the service is enabled, that is, the Enable check box is selected.

➢ **To edit or delete a port triggering entry:**

1. Select **Advanced > Advanced Setup > Port Forwarding / Port Triggering**.

   The Port Forwarding / Port Triggering screen displays.

2. Select the **Port Triggering** radio button.

   The screen adjusts to display the port triggering information.

3. In the Port Triggering Portmap Table, select the radio button next to the service that you want to edit or delete.

4. Do one of the following:
   - Click the **Edit Service** button.

     The Port Triggering - Services screen displays.

     a. Edit the service.

     b. Click the **Apply** button.
   - Click the **Delete Service** button.

     The service is removed from the table.

Dynamic DNS

If your Internet service provider (ISP) gave you a permanently assigned IP address, you can register a domain name and have that name linked with your IP address by public Domain Name Servers (DNS). However, if your Internet account uses a dynamically assigned IP address, you do not know in advance what your IP address will be, and the address can change frequently. In this case, you can use a commercial Dynamic DNS service. This type of service lets you register your domain to their IP address and forwards traffic directed at your domain to your frequently changing IP address.

If your ISP assigns a private WAN IP address (such as 192.168.x.x or 10.x.x.x), the Dynamic DNS service does not work because private addresses are not routed on the Internet.

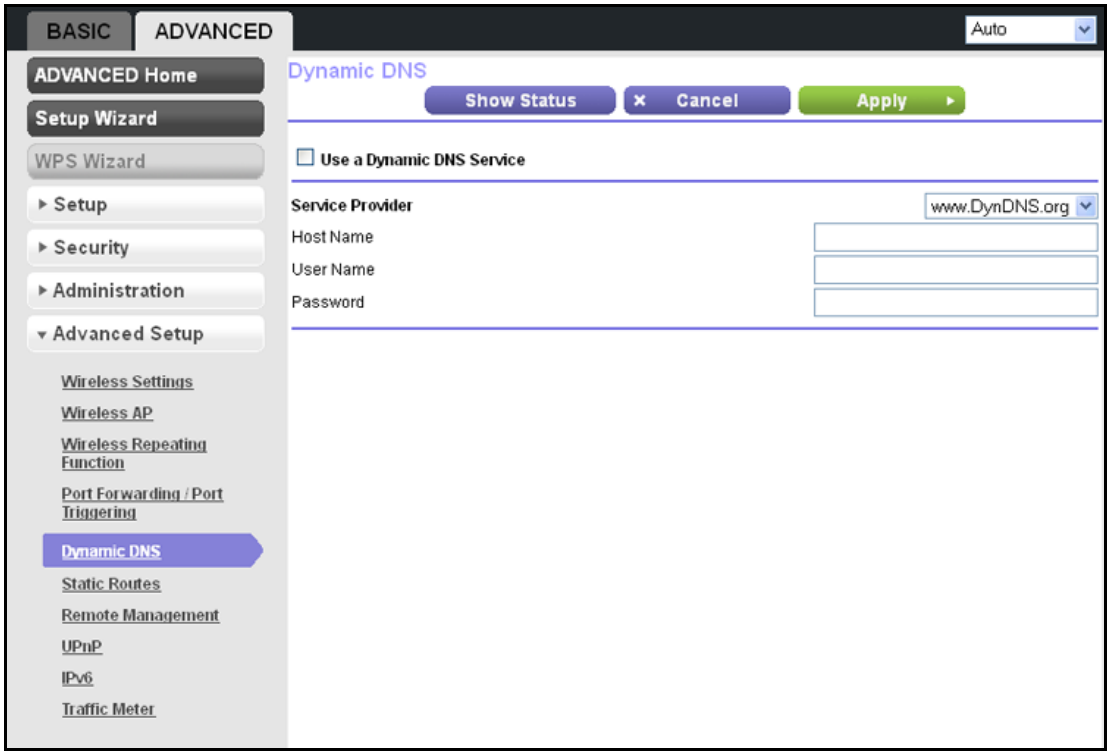
Your router contains a client that can connect to the Dynamic DNS service provided by DynDNS.org. First visit their website at *http://www.dyndns.org* and obtain an account and host name that you configure in the router. Then, whenever your ISP-assigned IP address changes, your router automatically contacts the Dynamic DNS service provider, logs in to your account, and registers your new IP address. If your host name is hostname, for example, you can reach your router at http://hostname.dyndns.org.

Note: Before you set up Dynamic DNS on router, first register an account with one of the Dynamic DNS service providers whose URLs appear in the Service Provider list on the Dynamic DNS screen.

➢ **To set up Dynamic DNS:**

1. Select **Advanced > Advanced Setup > Dynamic DNS**.

   The Dynamic DNS screen displays:



2. Select the **Use a Dynamic DNS Service** check box.
3. Select the URL of your Dynamic DNS service provider.
4. Type the host name (or domain name) that your Dynamic DNS service provider gave you.
5. Type the user name for your Dynamic DNS account.

   This is the name that you use to log in to your account, not your host name.
6. Type the password (or key) for your Dynamic DNS account.
7. Click the **Apply** button.
8. (Optional) To verify the Dynamic DNS status, click the **Show Status** button.

Static Routes

Static routes provide additional routing information to your router. Under usual circumstances, the router has adequate routing information after it has been configured for Internet access, and you do not need to configure additional static routes. You have to configure static routes only for unusual cases such as multiple routers or multiple IP subnets located on your network.

As an example of when a static route is needed, consider the following case:

- Your primary Internet access is through a cable modem to an ISP.
- You have an ISDN router on your home network for connecting to the company where you are employed. This router's address on your LAN is 192.168.1.100.
- Your company's network address is 134.177.0.0.

When you first configured your router, two implicit static routes were created. A default route was created with your ISP as the gateway, and a second static route was created to your local network for all 192.168.1.x addresses. With this configuration, if you attempt to access a device on the 134.177.0.0 network, your router forwards your request to the ISP. The ISP forwards your request to the company where you are employed, and the request is likely to be denied by the company's firewall.

In this case you have to define a static route, telling your router that 134.177.0.0 should be accessed through the ISDN router at 192.168.1.100. In this example:

- The Destination IP Address and IP Subnet Mask fields specify that this static route applies to all 134.177.x.x addresses.
- The Gateway IP Address field specifies that all traffic for these addresses should be forwarded to the ISDN router at 192.168.1.100.
- A metric value of 1 works because the ISDN router is on the LAN.
- Private is selected only as a precautionary security measure in case RIP is activated.

➢ **To set up a static route:**

1. Select **Advanced > Advanced Setup > Static Routes**.

   The Static Routes screen displays.

2. Click the **Add** button.

The screen adjusts:

3. In the Route Name field, type a name for this static route (for identification purposes only.)
4. Select the **Private** check box if you want to limit access to the LAN only. If you select Private, the static route is not reported in RIP.
5. Select the **Active** check box to make this route effective. (By default, the Active check box is selected.)
6. Type the IP address of the final destination.
7. Type the IP subnet mask for this destination. If the destination is a single host, type **255.255.255.255**.
8. Type the gateway IP address, which has to be a router on the same LAN segment as the N300 Wireless Router.
9. Type a number between 1 and 15 as the metric value.

   This value represents the number of routers between your network and the destination. Usually, a setting of 2 or 3 works, but if this is a direct connection, set it to 1.
10. Click the **Apply** button.

    The route is added to the table on the Static Routes screen.

➢ **To edit or delete a static route:**

1. Select **Advanced > Advanced Setup > Static Routes**.

   The Static Routes screen displays.
2. In the table, select the radio button next to the route that you want to edit or delete.

3. Do one of the following:
   - Click the **Edit** button.

     The Static Routes screen adjusts.

     a. Edit the route information.

     b. Click the **Apply** button.
   - Click the **Delete** button.

     The route is removed from the table.

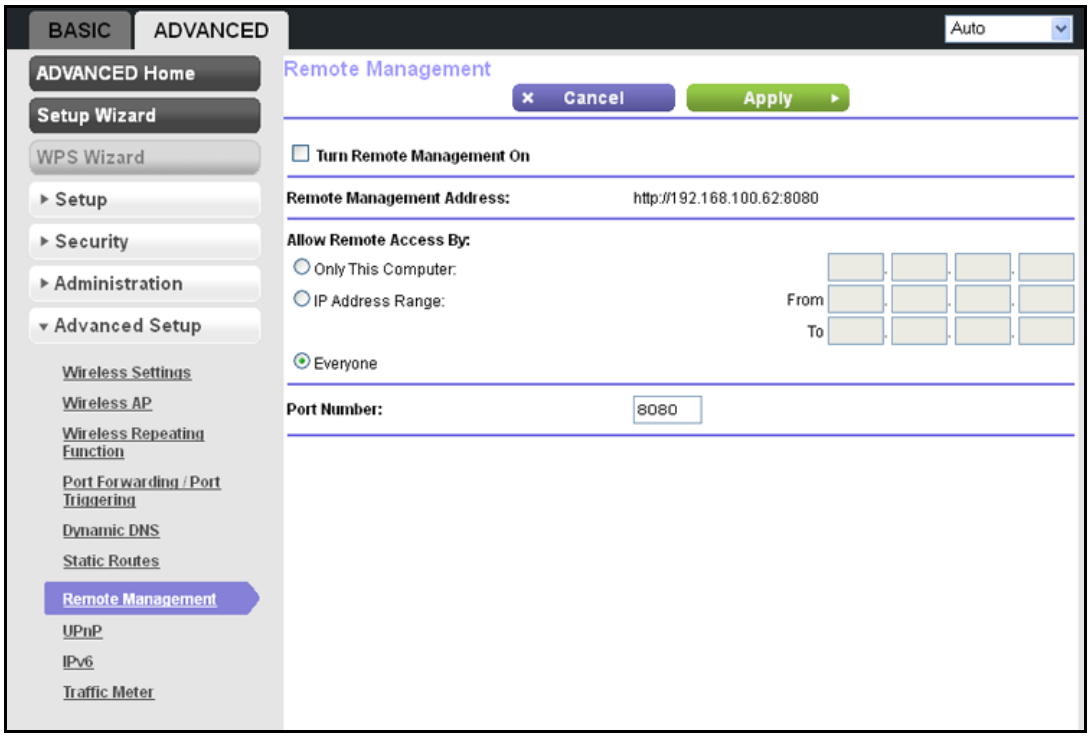
Remote Management

The remote management feature lets you upgrade or check the status of your router over the Internet.

Note: Before you enable remote management, be sure to change the router's default login password to a very secure password. The ideal password should contain no dictionary words from any language and contain uppercase and lowercase letters, numbers, and symbols. It can be up to 30 characters.

➢ **To set up remote management:**

1. Select **Advanced > Advanced Setup > Remote Management**.



2. Select the **Turn Remote Management On** check box.
3. Under Allow Remote Access By, specify the external IP addresses to be allowed to access the router's remote management.

   Note: *For enhanced security, restrict access to as few external IP addresses as practical.*

   - To allow access from a single IP address on the Internet, select the **Only This Computer** radio button. Enter the IP address that is allowed access.
   - To allow access from a range of IP addresses on the Internet, select the **IP Address Range** radio button. Enter a beginning and ending IP address to define the allowed range.
   - To allow access from any IP address on the Internet, select the **Everyone** radio button.
4. Specify the port number for accessing the router user interface.

   Normal web browser access uses the standard HTTP service port 80. For greater security, enter a custom port number for the remote router user interface. Choose a number between 1024 and 65535, but do not use the number of any common service port. The default is 8080, which is a common alternate for HTTP.
5. Click the **Apply** button.

When you access your router from the Internet, type your router's WAN IP address in your browser's address or location field followed by a colon (:) and the custom port number. For example, if your external address is 203.0.113.123 and you use port number 8080, enter **http://203.0.113.123:8080** in your browser.

Universal Plug and Play

Universal Plug and Play (UPnP) helps devices, such as Internet appliances and computers, to access the network and connect to other devices as needed. UPnP devices can automatically discover the services from other registered UPnP devices on the network.

Note: If you use applications such as multiplayer gaming, peer-to-peer connections, or real-time communications such as instant messaging or remote assistance, you should enable UPnP.

➢ **To turn on Universal Plug and Play:**

1. Select **Advanced > Advanced Setup > UPnP**.

The UPnP screen displays.

2. Select the **Turn UPnP On** check box.

   By default, this check box is selected. UPnP can be enabled or disabled for automatic device configuration. If the Turn UPnP On check box is cleared, the router does not allow any device to automatically control the resources, such as port forwarding (mapping) of the router.

3. Type the advertisement period in minutes.

   The advertisement period specifies how often the router broadcasts its UPnP information. This value can range from 1 to 1440 minutes. The default period is 30 minutes. Shorter durations ensure that control points have current device status at the expense of additional network traffic. Longer durations can compromise the freshness of the device status, but can significantly reduce network traffic.

4. Type the advertisement time to live in hops.

   The time to live for the advertisement is measured in hops (steps) for each UPnP packet sent. The time to live hop count is the number of steps a broadcast packet is allowed to propagate for each UPnP advertisement before it disappears. The number of hops can range from 1 to 255. The default value for the advertisement time to live is 4 hops, which should be fine for most home networks. If you notice that some devices are not being updated or reached correctly, it might be necessary to increase this value.

5. Click the **Apply** button.

   The UPnP Portmap Table displays the IP address of each UPnP device that is accessing the router and which ports (internal and external) that device has opened. The UPnP

Portmap Table also displays what type of port is open and whether that port is still active for each IP address.

6. (Optional) To refresh the information in the UPnP Portmap Table, click the **Refresh** button.

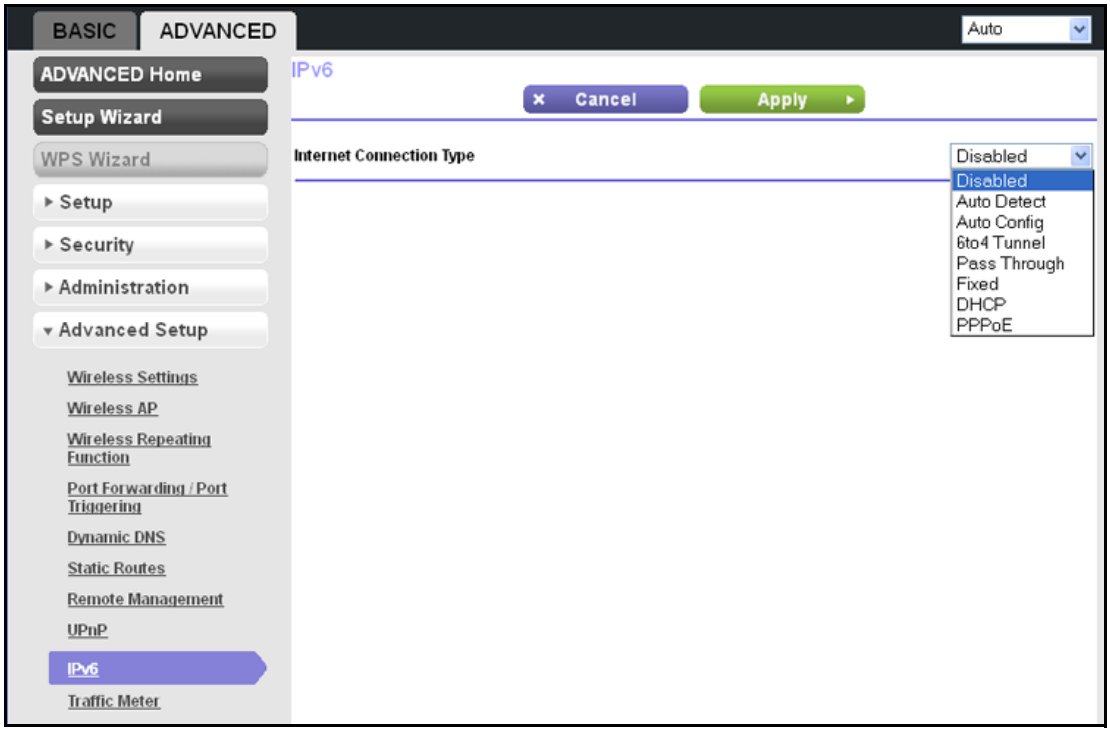
IPv6

You can use this feature to set up an IPv6 Internet connection type if NETGEAR genie does not detect it automatically.

➢ **To set up an IPv6 Internet connection type:**

1. Select **Advanced > Advanced Setup > IPv6**.

   The IPv6 screen displays:



2. Select the IPv6 connection type from the list. Your Internet service provider (ISP) can provide this information.
   - If your ISP did not provide details, you can select **6to4 Tunnel**.
   - If you are not sure what type of IPv6 connection the router uses, select **Auto Detect** so that the router detects the IPv6 type that is in use.
   - If your Internet connection does not use PPPoE, DHCP, a fixed IP address, or pass-through but is IPv6, select **Auto Config**.

Note: For IPv6 address requirements and detailed information about IPv6 Internet connection types, see the following sections.

3. Click the **Apply** button.

Requirements for Entering IPv6 Addresses

IPv6 addresses are denoted by eight groups of hexadecimal quartets that are separated by colons. Any four-digit group of zeroes within an IPv6 address can be reduced to a single zero or altogether omitted.

The following errors invalidate an IPv6 address:

- More than eight groups of hexadecimal quartets
- More than four hexadecimal characters in a quartet
- More than two colons in a row

IPv6 Auto Detect

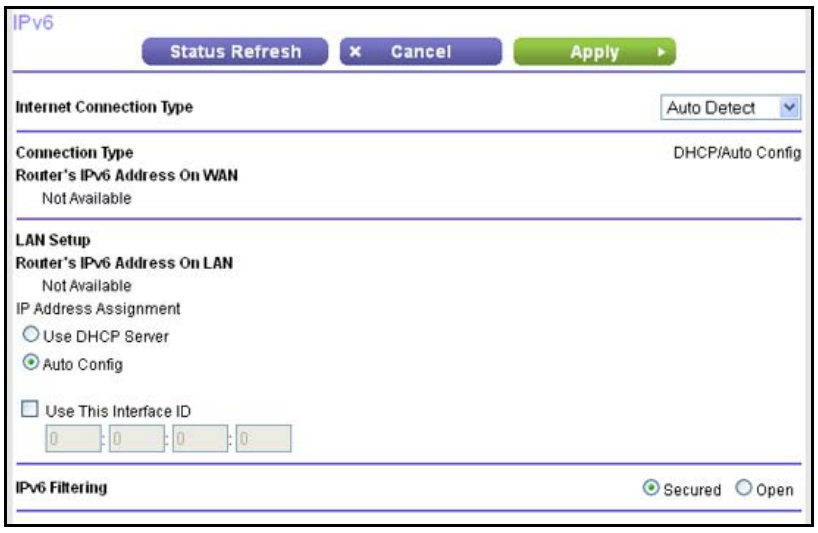
➢ **To set up an IPv6 Internet connection through auto detection:**

1. Select **Advanced > Advanced Setup > IPv6**.

   The IPv6 screen displays.

2. Select **Auto Detect** from the menu.

   The screen adjusts:



The information in the following fields is automatically detected by the router:

- **Connection Type**. This field indicates the connection type that is detected.
- **Router's IPv6 Address on WAN**. This field shows the IPv6 address that is acquired for the router's WAN (or Internet) interface. The number after the slash (/) is the length of the prefix, which is also indicated by the underline (_) under the IPv6 address. If no address is acquired, the field displays Not Available.
- **Router's IPv6 Address on LAN**. This field shows the IPv6 address that is acquired for the router's LAN interface. The number after the slash (/) is the length of the prefix, which is also indicated by the underline (_) under the IPv6 address. If no address is acquired, the field displays Not Available.

3. Specify how the router assigns IPv6 addresses to the devices on your home network (the LAN) by selecting one of the following radio buttons:
   - **Use DHCP Server**. This method passes more information to LAN devices, but some IPv6 systems might not support the DHCv6 client function.
   - **Auto Config**. This is the default setting.
4. (Optional) Select the **Use This Interface ID** check box, and specify the interface ID that you want to be used for the IPv6 address of the router's LAN interface.

   If you do not specify an ID here, the router generates one automatically from its MAC address.
5. Specify IPv6 filtering.

   When the connection type is not IPv6 Pass Through or Disabled, the router starts the stateful packet inspection (SPI) firewall function on the WAN interface. The router creates connection records and checks every inbound IPv6 packet. If the inbound packet is not destined to the router itself and the router does not expect to receive such a packet, or the packet is not in the connection record, the router blocks this packet. This function has two modes.

   Specify the mode by selecting one of the following radio buttons:
   - **Secured**. In the secured mode, which is the default mode, the router inspects both TCP and UDP packets.
   - **Open**. In the open mode, the router inspects UDP packets only.
6. Click the **Apply** button.

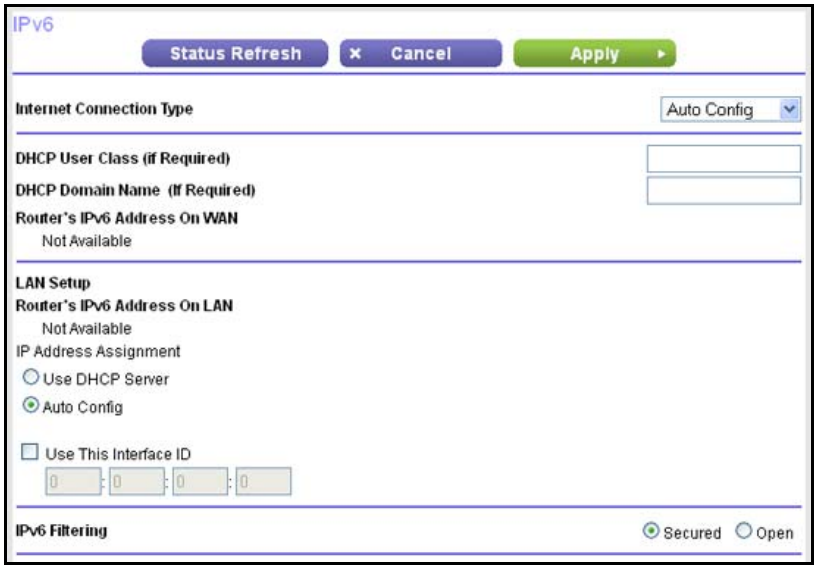
IPv6 Auto Config

➢ **To set up an IPv6 Internet connection through auto configuration:**

1. Select **Advanced > Advanced Setup > IPv6**.

   The IPv6 screen displays.
2. Select **Auto Config** from the menu.

The screen adjusts:



The information in the following fields is automatically detected by the router:

- **Router's IPv6 Address on WAN**. This field shows the IPv6 address that is acquired for the router's WAN (or Internet) interface. The number after the slash (/) is the length of the prefix, which is also indicated by the underline (_) under the IPv6 address. If no address is acquired, the field displays Not Available.
- **Router's IPv6 Address on LAN**. This field shows the IPv6 address that is acquired for the router's LAN interface. The number after the slash (/) is the length of the prefix, which is also indicated by the underline (_) under the IPv6 address. If no address is acquired, the field displays Not Available.

3. (Optional) In the DHCP User Class (If Required) field, enter a host name.

   Most people do not need to fill in this field, but if your ISP has given you a specific host name, enter it here.

4. (Optional) In the Domain Name (If Required) field, enter a domain name.

   You can type the domain name of your IPv6 ISP. (Do not enter the domain name for the IPv4 ISP here.) For example, if your ISP's mail server is mail.xxx.yyy.zzz, you would type xxx.yyy.zzz as the domain name. If your ISP provided a domain name, type it in this field. (For example, Earthlink Cable might require a host name of home, and Comcast sometimes supplies a domain name.)

5. Configure the LAN setup and IPv6 filtering settings as explained in *Step 3* through *Step 5* of the procedure to set up an IPv6 Internet connection through auto detection (see *IPv6 Auto Detect* on page 104).
6. Click the **Apply** button.

IPv6 6to4 Tunnel

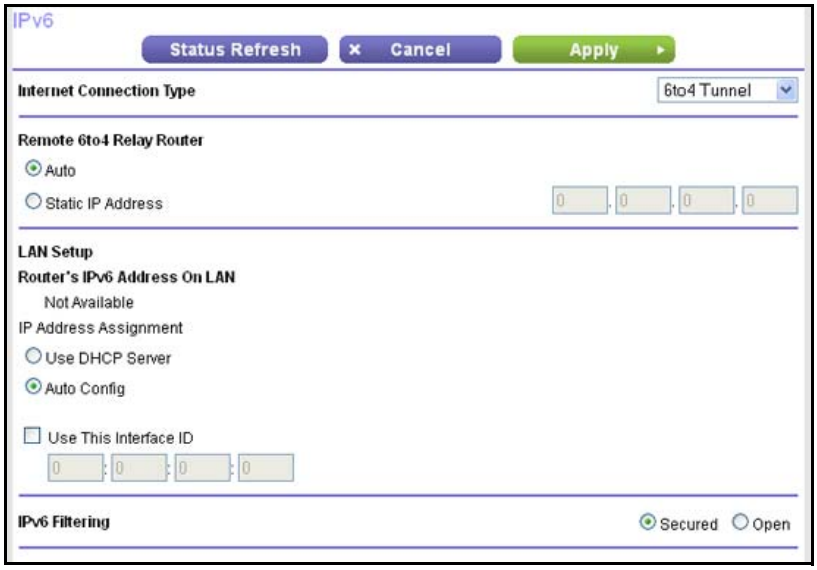
➢ **To set up an IPv6 Internet connection by using a 6to4 tunnel:**

1. Select **Advanced > Advanced Setup > IPv6**.

   The IPv6 screen displays.

2. Select **6to4 Tunnel** from the menu.

   The screen adjusts:



   The information in the following fields is automatically detected by the router:

   - **Router's IPv6 Address on WAN**. This field shows the IPv6 address that is acquired for the router's WAN (or Internet) interface. The number after the slash (/) is the length of the prefix, which is also indicated by the underline (_) under the IPv6 address. If no address is acquired, the field displays Not Available.
   - **Router's IPv6 Address on LAN**. This field shows the IPv6 address that is acquired for the router's LAN interface. The number after the slash (/) is the length of the prefix, which is also indicated by the underline (_) under the IPv6 address. If no address is acquired, the field displays Not Available.

3. Configure the remote 6to4 relay router settings by selecting one of the following radio buttons:

   - **Auto**. Your router uses any remote relay router that is available on the Internet.

     This is the default setting.

   - **Static IP Address**. Enter the static IPv4 address of the remote relay router.

     This address is usually provided by your IPv6 ISP.

   Note: The remote relay router is the router to which your router creates the 6to4 tunnel. Make sure that the IPv4 Internet connection is working before your apply the 6to4 tunnel settings for the IPv6 connection.

4. Configure the LAN setup and IPv6 filtering settings as explained in *Step 3* through *Step 5* of the procedure to set up an IPv6 Internet connection through auto detection (see *IPv6 Auto Detect* on page 104).
5. Click the **Apply** button.

IPv6 Pass Through

In pass-through mode, the router works as a Layer 2 Ethernet switch with two ports (LAN and WAN Ethernet ports) for IPv6 packets. The router does not process any IPv6 header packets.

➢ **To set up a pass-through IPv6 Internet connection:**

1. Select **Advanced > Advanced Setup > IPv6**.

   The IPv6 screen displays.
2. Select **Pass Through** from the menu.

   The screen adjusts, but no additional fields display.
3. Click the **Apply** button.

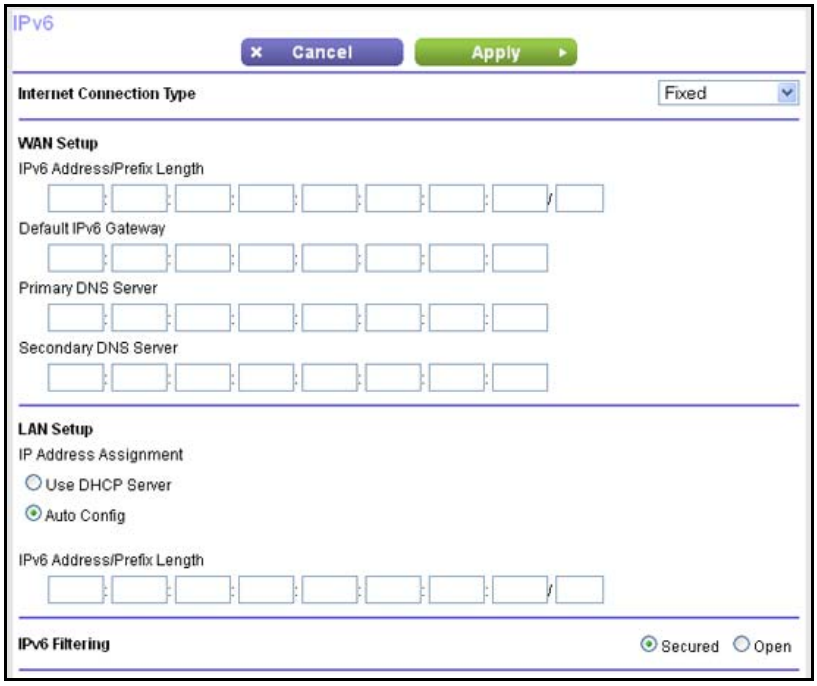
IPv6 Fixed

➢ **To set up an IPv6 Internet connection with a fixed IPv6 address:**

1. Select **Advanced > Advanced Setup > IPv6**.

   The IPv6 screen displays.
2. Select **Fixed** from the menu.

The screen adjusts:



3. Configure the fixed IPv6 addresses for the WAN connection:
   - **IPv6 Address/Prefix Length**. The static IPv6 address and prefix length of the router's WAN interface.
   - **Default IPv6 Gateway**. The IPv6 address of the default IPv6 gateway.
   - **Primary DNS Server**. The primary DNS server that resolves IPv6 domain name records for the router.
   - **Secondary DNS Server**. The secondary DNS server that resolves IPv6 domain name records for the router.

   Note: *If you do not specify the DNS servers, the router uses the DNS servers that are configured for the IPv4 Internet connection on the Internet Setup screen (see Internet Setup on page 24).*

4. Specify how the router assigns IPv6 addresses to the devices on your home network (the LAN) by selecting one of the following radio buttons:
   - **Use DHCP Server**. This method passes more information to LAN devices, but some IPv6 systems might not support the DHCv6 client function.
   - **Auto Config**. This is the default setting.
5. In the IPv6 Address/Prefix Length field, specify the static IPv6 address and prefix length of the router's LAN interface.

   If you do not specify an ID here, the router generates one automatically from its MAC address.
6. Specify IPv6 filtering.

When the connection type is not IPv6 Pass Through or Disabled, the router starts the stateful packet inspection (SPI) firewall function on the WAN interface. The router creates connection records and checks every inbound IPv6 packet. If the inbound packet is not destined to the router itself and the router does not expect to receive such a packet, or the packet is not in the connection record, the router blocks this packet. This function has two modes.

Specify the mode by selecting one of the following radio buttons:

- **Secured**. In the secured mode, which is the default mode, the router inspects both TCP and UDP packets.
- **Open**. In the open mode, the router inspects UDP packets only.

7. Click the **Apply** button.

IPv6 DHCP

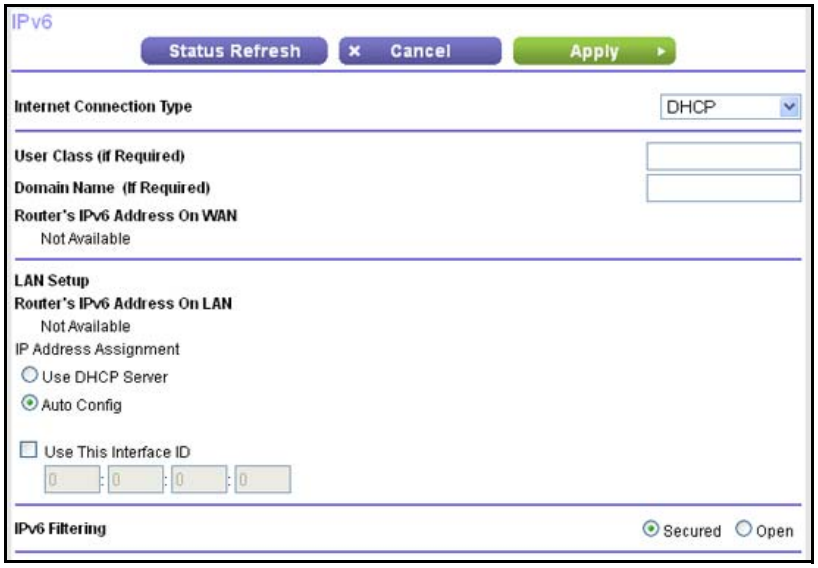
➢ **To set up an IPv6 Internet connection with a DHCP server:**

1. Select **Advanced > Advanced Setup > IPv6**.

   The IPv6 screen displays.

2. Select **DHCP** from the menu.

   The screen adjusts:



   The information in the following fields is automatically detected by the router:

   - **Router's IPv6 Address on WAN**. This field shows the IPv6 address that is acquired for the router's WAN (or Internet) interface. The number after the slash (/) is the length of the prefix, which is also indicated by the underline (_) under the IPv6 address. If no address is acquired, the field displays Not Available.

- **Router's IPv6 Address on LAN**. This field shows the IPv6 address that is acquired for the router's LAN interface. The number after the slash (/) is the length of the prefix, which is also indicated by the underline (_) under the IPv6 address. If no address is acquired, the field displays Not Available.

3. (Optional) In the DHCP User Class (If Required) field, enter a host name.

   Most people do not need to fill in this field, but if your ISP has given you a specific host name, enter it here.

4. (Optional) In the Domain Name (If Required) field, enter a domain name.

   You can type the domain name of your IPv6 ISP. (Do not enter the domain name for the IPv4 ISP here.) For example, if your ISP's mail server is mail.xxx.yyy.zzz, you would type xxx.yyy.zzz as the domain name. If your ISP provided a domain name, type it in this field. (For example, Earthlink Cable might require a host name of home, and Comcast sometimes supplies a domain name.)

5. Configure the LAN setup and IPv6 filtering settings as explained in *Step 3* through *Step 5* of the procedure to set up an IPv6 Internet connection through auto detection (see *IPv6 Auto Detect* on page 104).
6. Click the **Apply** button.

IPv6 PPPoE

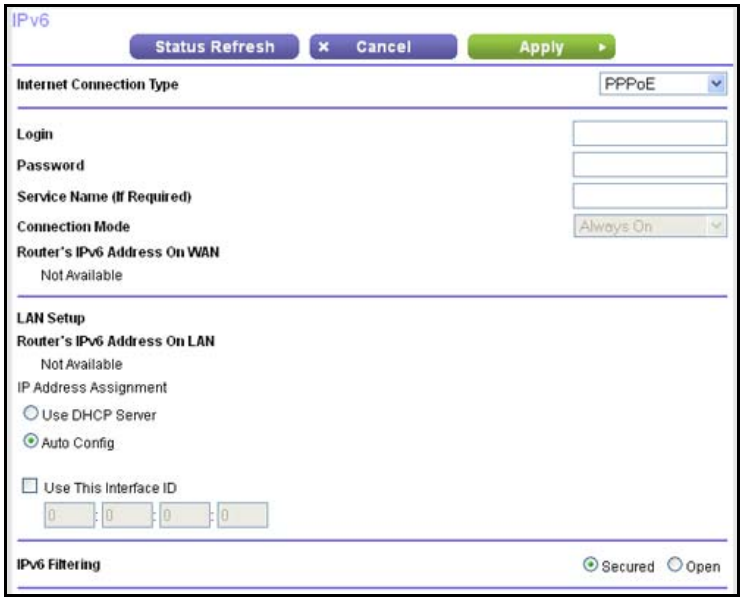
➢ **To set up a PPPoE IPv6 Internet connection:**

1. Select **Advanced > Advanced Setup > IPv6**.

   The IPv6 screen displays.

2. Select **PPPoE** from the menu.

   The screen adjusts:



The information in the following fields is automatically detected by the router:

- **Router's IPv6 Address on WAN**. This field shows the IPv6 address that is acquired for the router's WAN (or Internet) interface. The number after the slash (/) is the length of the prefix, which is also indicated by the underline (_) under the IPv6 address. If no address is acquired, the field displays Not Available.
- **Router's IPv6 Address on LAN**. This field shows the IPv6 address that is acquired for the router's LAN interface. The number after the slash (/) is the length of the prefix, which is also indicated by the underline (_) under the IPv6 address. If no address is acquired, the field displays Not Available.

3. In the Login fields, enter the login information for the ISP connection.

   This is usually the name that you use in your email address. For example, if your main mail account is JerAB@ISP.com, then you would type JerAB in this field. Some ISPs (like Mindspring, Earthlink, and T-DSL) require that you use your full email address when you log in. If your ISP requires your full email address, type it in this field.

4. In the Password field, enter the password for the ISP connection.
5. In the Service Name name field, enter a service name.

   If your ISP did not provide a service name, leave this field blank.

   Note: *The default setting of the Connection Mode field is Always on to provide a steady IPv6 connection. The router never terminates the connection. If the connection is terminated, for example, when the modem is turned off, the router attempts to reestablish the connection immediately after the PPPoE connection becomes available again.*

6. Configure the LAN setup and IPv6 filtering settings as explained in *Step 3* through *Step 5* of the procedure to set up an IPv6 Internet connection through auto detection (see *IPv6 Auto Detect* on page 104).
7. Click the **Apply** button.

Traffic Meter

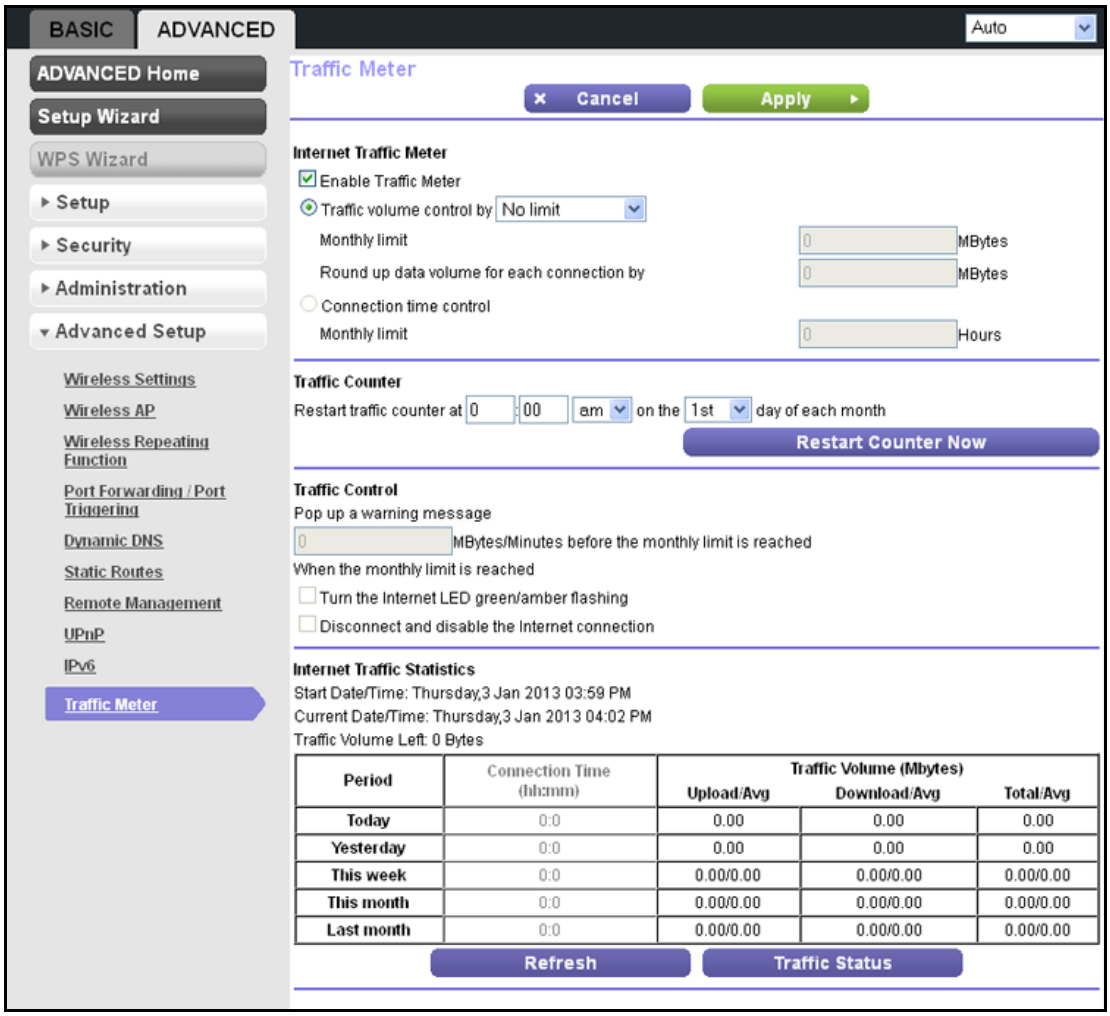
Traffic metering allows you to monitor the volume of Internet traffic passing through your router's Internet port. With the traffic meter utility, you can set limits for traffic volume, set a monthly limit, and get a live update of traffic usage.

➢ **To start monitoring Internet traffic:**

1. Select **Advanced > Advanced Setup > Traffic Meter**.

   The Traffic Meter screen displays.

2. To enable the traffic meter, select the **Enable Traffic Meter** check box.



3. If you would like to record and restrict the volume of Internet traffic, select the **Traffic volume control by** radio button. You can select one of the following options for controlling the traffic volume:
   - **No Limit**. No restriction is applied when the traffic limit is reached.
   - **Download only**. The restriction is applied to incoming traffic only.
   - **Both Directions**. The restriction is applied to both incoming and outgoing traffic.
4. In the Monthly Limit field, enter how many MBytes (MB) per month are allowed.

   Instead of MB, you can also specify how many hours of traffic are allowed by selecting the **Connection time control** radio button and entering the allowed hours in the Monthly limit field.
5. (Optional) If your ISP charges an amount of extra data volume when you make a new connection, enter the extra data volume in MB in the Round up data volume for each connection by field.
6. In the Traffic Counter section, set up the traffic counter to begin at a specific time and date of each month.

If you want the traffic counter to start immediately, click the **Restart Counter Now** button.

7. In the Traffic Control section, specify whether a warning message is issued before the monthly traffic limit of MB or hours is reached.

   By default, the value is 0 and no warning message is issued. You can select one of the following to occur when the traffic limit is reached:

   - The Internet LED flashes green or amber.
   - The Internet connection is disconnected and disabled.

8. Click the **Apply** button.

The Internet Traffic Statistics section helps you to monitor the data traffic.

Click the **Refresh** button to update the Traffic Statistics section.

Click the **Traffic Status** button to display more information about the data traffic on your router and to change the poll interval.

Monitoring

8

Monitor your router and network traffic

This chapter describes how to monitor your the router and network traffic. This chapter includes the following sections:

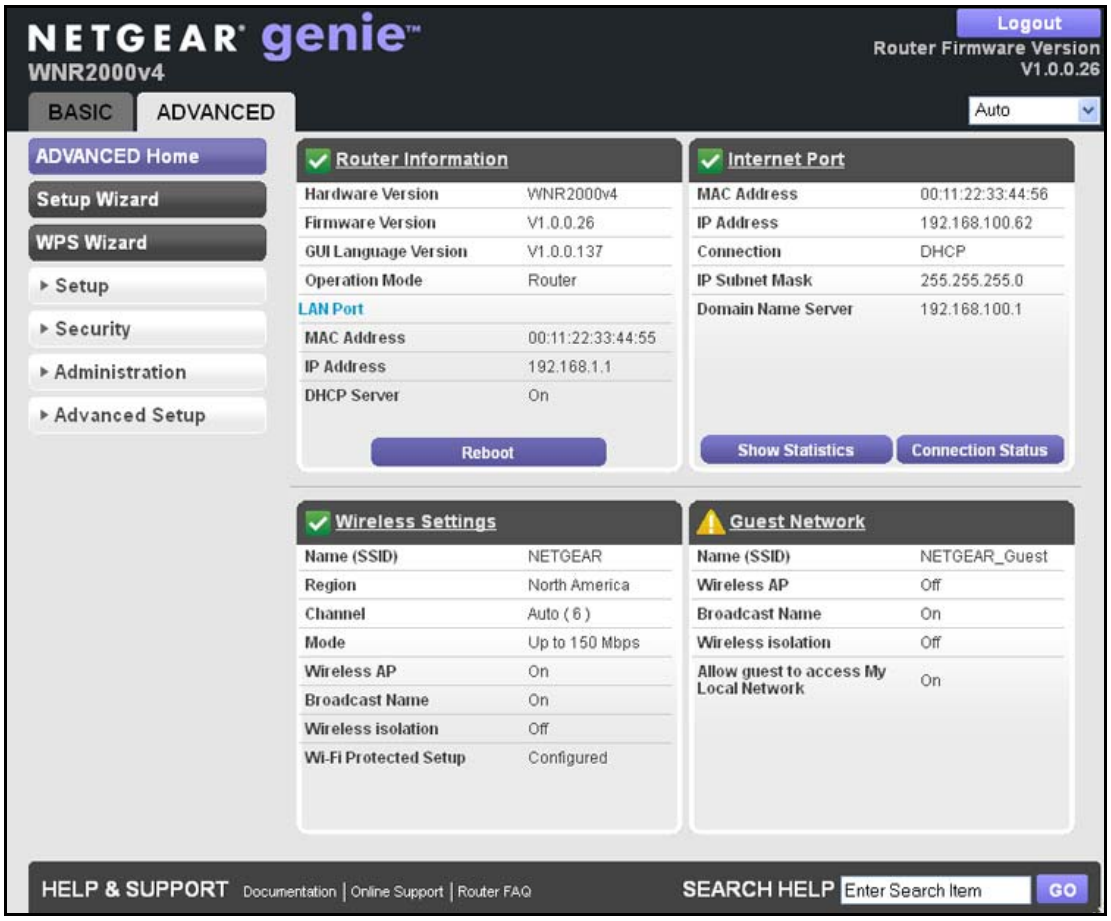
- *Router Status and Usage Information Screen*
- *Router Information Pane*
- *Internet Port Pane*
- *Wireless Settings Pane*
- *Guest Network Pane*

Router Status and Usage Information Screen

➢ **To view router status and usage information:**

Select **Advanced**.

The screen that displays shows information about the router, the Internet port, the wireless settings, and the guest network (this screen is referred to as the Router Status screen):



Note: The Router Status screen also displays when you select **Advanced > Advanced Home** or **Advanced > Administration > Router Status**.

Router Information Pane

➢ **To display the Router Information pane:**

Select the **Advanced** tab.

The Router Status screen displays. The Router Information pane is located in the upper left of the screen.

The following settings are displayed:

Hardware Version. The router model.

Firmware Version. The version of the router firmware. It changes if you upgrade the router firmware.

GUI Language Version. The localized language of the router user interface.

Operation Mode. The mode in which the router operates:

- **Router**. The router functions in default mode.
- **AP**. The router functions as an access point only.

LAN Port.

- **MAC Address**. The Media Access Control address for the LAN port. This is the unique physical address being used by the Ethernet (LAN) port of the router.
- **IP Address**. The IP address that is used by the Ethernet (LAN) port of the router. The default is 192.168.1.1.
- **DHCP Server**. Identifies whether the router's built-in DHCP server is active for the LAN-attached devices.

Internet Port Pane

➢ **To display the Internet Port pane:**

Select the **Advanced** tab.

The Router Status screen displays. The Internet Port pane is located in the upper right of the screen.

The following settings are displayed:

MAC Address. The Media Access Control (MAC) address for the Internet port. This is the unique physical address being used by the Internet (WAN) port of the router.

IP Address. The IP address that is used by the Internet (WAN) port of the router. If no address is shown or the address is 0.0.0, the router is not connected to the Internet.

Connection. Shows whether the router is using a fixed or dynamic IP address on the Internet port. If the value is DHCP, the router obtains an IP address dynamically from the ISP or from a DHCP server on your LAN.

IP Subnet Mask. The IP subnet mask that is used by the Internet port of the router.

Domain Name Server. The Domain Name Server address that is used by the router. A Domain Name Server translates human-language URLs such as www.netgear.com into IP addresses.

Statistics

The router provides a variety of statistics.

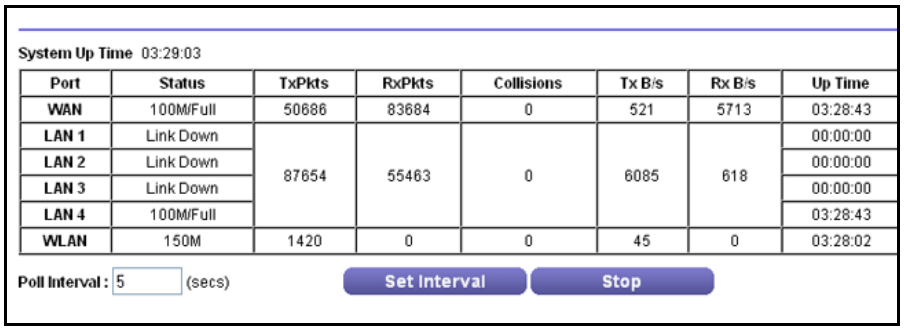
➢ **To view the traffic statistics:**

1. Select the **Advanced** tab.

   The Router Status screen displays.

2. In the Internet Port pane, click the **Show Statistics** button.

   A pop-up screen displays traffic statistics:



System Up Time 03:29:03

Port	Status	TxPkts	RxPkts	Collisions	Tx B/s	Rx B/s	Up Time
WAN	100M/Full	50686	83684	0	521	5713	03:28:43
LAN 1	Link Down	87654	55463	0	6085	618	00:00:00
LAN 2	Link Down						00:00:00
LAN 3	Link Down						00:00:00
LAN 4	100M/Full						03:28:43
WLAN	150M	1420	0	0	45	0	03:28:02

Poll Interval : 5 (secs) Set Interval Stop

The following settings are displayed:

System Up Time. The time elapsed since the router was last restarted.

Port. The statistics for the WAN (Internet) port, the four LAN (Ethernet) ports combined, and the wireless LAN (WLAN) port.

Status. The link status of the port.

TxPkts. The number of packets transmitted on this port since reset or manual clear.

RxPkts. The number of packets received on this port since reset or manual clear.

Collisions. The number of collisions on this port since reset or manual clear.

Tx B/s. The current transmission (outbound) bandwidth that is used on the port.

Rx B/s. The current reception (inbound) bandwidth that is used on the port.

Up Time. The time elapsed since the port acquired the link.

Poll Interval. The interval at which the statistics are updated on this screen.

To change the polling frequency, enter a time in seconds in the Poll Interval field, and click the **Set Interval** button.

To stop the polling entirely, click the **Stop** button.

Connection Status

The content of this screen depends on the type of connection. For example, different information is shown for a PPPoE connection than for a DHCP connection.

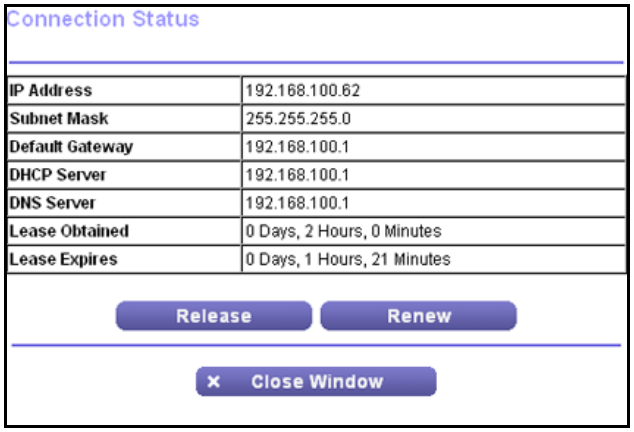
➢ **To view the connection status:**

1. Select the **Advanced** tab.

   The Router Status screen displays.

2. In the Internet Port pane, click the **Connection Status** button.

   The Connection Status pop-up screen displays. The following figure shows the connection status information for a DHCP connection.



   The following sections describe the different types of connections and the associated settings that are displayed on the Connection Status pop-up screen.

DHCP Connection

The content of the Connection Status pop-up screen depends on the type of connection.

The following settings are displayed for a DHCP connection:

- **IP Address**. The IP address that is assigned to the router.
- **Subnet Mask**. The subnet mask that is assigned to the router.
- **Default Gateway**. The IP address for the default gateway that the router communicates with.
- **DHCP Server**. The IP address for the Dynamic Host Configuration Protocol server that provides the TCP/IP configuration for all the computers that are connected to the router.
- **DNS Server**. The IP address of the Domain Name Service server that provides translation of network names to IP addresses.
- **Lease Obtained**. The date and time when the lease was obtained.
- **Lease Expires**. The date and time that the lease expires.

Click the **Release** button to release the router's IP address and terminate the Internet connection.

Click the **Renew** button to let the router acquire an IP address from the DHCP server and start the Internet connection.

Click the **Close Window** button to close the Connection Status screen.

PPPoE Connection

The content of the Connection Status pop-up screen depends on the type of connection.

The following settings are displayed for a PPPoE connection:

- **Connection Time**. The time that has elapsed since the connection was established.
- **Connection Status**. The status of the connection: Connected, Disconnected, Negotiation (---, Success), or Authentication (---, Success). Note that --- indicates failure.
- **IP Address**. The IP address that is assigned to the router.
- **Subnet Mask**. The subnet mask that is assigned to the router.

Click the **Connect** button to establish the PPPoE connection manually.

Click the **Disconnect** button to terminate the PPPoE connection manually.

Click the **Close Window** button to close the Connection Status screen.

PPTP Connection

The content of the Connection Status pop-up screen depends on the type of connection.

The following settings are displayed for a PPTP connection:

- **Connection Status**. The status of the connection: Connected or Disconnected.
- **IP Address**. The IP address that is assigned to the router.
- **Subnet Mask**. The subnet mask that is assigned to the router.

Click the **Connect** button to establish the PPTP connection manually.

Click the **Disconnect** button to terminate the PPTP connection manually.

Click the **Close Window** button to close the Connection Status screen.

Wireless Settings Pane

➢ **To display the Wireless Settings pane:**

Select the **Advanced** tab.

The Router Status screen displays. The Wireless Settings pane is located in the lower left of the screen.

The following settings are displayed:

Name (SSID). The wireless network name (SSID) that is used by the router.

Region. The geographic region where the router is used. It might be illegal to use the wireless features of the router in some parts of the world.

Channel. Identifies the operating channel of the wireless port. The default channel is Auto. When Auto is selected, the router finds the best operating channel available. If you notice interference from nearby devices, you can select a different channel. Channels 1, 6, and 11 do not interfere with each other.

Mode. Indicates the wireless communication mode: Up to 54 Mbps, Up to 150 Mbps (default), or Up to 300 Mbps.

Wireless AP. Indicates whether the radio of the router is enabled. If the radio is not enabled, the Wireless LED on the front panel is off.

Broadcast Name. Indicates whether the router is broadcasting its SSID.

Wireless Isolation. Indicates whether wireless isolation is on or off. When it is off, wireless clients (computers or wireless devices) that join the network can use the Internet, but cannot access each other or access Ethernet devices on the network.

Wi-Fi Protected Setup. Indicates whether Wi-Fi Protected Setup is configured for this network.

Guest Network Pane

➢ **To display the Guest Network pane:**

Select the **Advanced** tab.

The Router Status screen displays. The Guest Network pane is located in the lower right of the screen.

The following settings are displayed:

Name (SSID). The wireless network name (SSID) that is used by the router. The default name is NETGEAR-Guest.

Wireless AP. Indicates whether the radio of the router is enabled for the guest network.

Broadcast Name. Indicates whether the router is broadcasting its SSID for the guest network.

Wireless Isolation. Indicates whether wireless isolation is on or off for the guest network. When it is off, wireless clients (computers or wireless devices) that join the guest network can use the Internet, but cannot access each other or access Ethernet devices on the network.

Allow guest to access My Local Network. Indicates whether wireless clients on the guest network can access your local network, instead of only the Internet and other wireless clients on the guest network.

Troubleshooting

9

This chapter provides information to help you diagnose and solve problems you might have with your router. If you do not find the solution here, check the NETGEAR support site at *http://support.netgear.com* for product and contact information.

This chapter contains the following sections:

- *Quick Tips*
- *Troubleshoot with the LEDs*
- *Cannot Log In to the Router*
- *Cannot Access the Internet*
- *Changes Not Saved*
- *Wireless Connectivity*
- *Troubleshoot Your Network Using the Ping Utility*

Quick Tips

This section describes tips for troubleshooting some common problems.

Sequence to Restart Your Network

➢ **Make sure to restart your network in this sequence:**

1. Turn off *and* unplug the cable or DSL broadband modem.
2. Turn off the router and computers.
3. Plug in the cable or DSL broadband modem and turn it on. Wait 2 minutes.
4. Turn on the router and wait 2 minutes.
5. Turn on the computers.

Check Ethernet Cable Connections

Make sure that the Ethernet cables are securely plugged in.

- The Internet LED on the router is lit if the Ethernet cable connecting the router and the modem is plugged in securely and the modem and router are turned on.
- For each powered-on computer connected to the router by an Ethernet cable, the corresponding numbered router LAN port LED is lit.

Wireless Settings

Make sure that the wireless settings in the computer and router match exactly.

- For a wirelessly connected computer, the wireless network name (SSID) and wireless security settings of the router and wireless computer need to match exactly.
- If you set up an access list in the Advanced Wireless Settings screen, you have to add each wireless computer's MAC address to the router's access list.

Network Settings

Make sure that the network settings of the computer are correct.

- Wired and wirelessly connected computers need to have network IP addresses on the same network as the router. The simplest way to do this is to configure each computer to obtain an IP address automatically using DHCP.
- Some cable modem service providers require you to use the MAC address of the computer initially registered on the account. You can view the MAC address in the Attached Devices screen (see *Attached Devices* on page 32).

Troubleshoot with the LEDs

After you turn on power to the router, the following sequence of events should occur:

1. When power is first applied, verify that the Power LED is on.
2. Verify that the Power LED turns amber within a few seconds, indicating that the self-test is running.
3. After approximately 30 seconds, verify that:
   - The Power LED is solid green.
   - The Internet LED is lit.
   - A numbered Ethernet port LED is on for any local port that is connected to a computer. This indicates that a link has been established to the connected device.

You can use the LEDs on the front panel of the router for troubleshooting.

Power LED Is Off or Blinking

- Make sure that the power cord is securely connected to your router and that the power adapter is securely connected to a functioning power outlet.
- Check that you are using the 12V DC, 1.5A power adapter that NETGEAR supplied for this product.
- If the Power LED blinks slowly and continuously, the router firmware is corrupted. This can happen if a firmware upgrade is interrupted, or if the router detects a problem with the firmware. If the error persists, you have a hardware problem. For recovery instructions, or help with a hardware problem, contact technical support at *www.netgear.com/support*.

Power LED Stays Amber

When the router is turned on, the Power LED turns amber for about 20 seconds and then turns green. If the LED does not turn green, the router has a problem.

If the Power LED is still amber 1 minute after you turn on power to the router:

1. Turn the power off and back on to see if the router recovers.
2. Press and hold the **Restore Factory Settings** button to return the router to its factory settings.

   For more information, see *Factory Settings* on page 133.

If the error persists, you might have a hardware problem and should contact technical support at *www.netgear.com/support*.

All LEDs Remain Lit after Startup

When the router is turned on, the LEDs light for about 10 seconds and then turn off. If all the LEDs stay lit, there is a fault within the router.

If all LEDs are still lit 1 minute after power-up:

- Turn the power off and back on to see if the router recovers.
- Press and hold the **Restore Factory Settings** button to return the router to its factory settings.

  For more information, see *Factory Settings* on page 133.

If the error persists, you might have a hardware problem and should contact technical support at *www.netgear.com/support*.

Internet or LAN Port LEDs Are Off

If either the LAN port LEDs or the Internet LED does not light when the Ethernet connection is made, check the following:

- Make sure that the Ethernet cable connections are secure at the router and at the modem or computer.
- Make sure that power is turned on to the connected modem or computer.
- Be sure that you are using the correct cable:

  When you connect the router's Internet port to a cable or DSL broadband modem, use the cable that was supplied with the cable or DSL broadband modem. This cable could be a standard straight-through Ethernet cable or an Ethernet crossover cable.

Wireless LED Is Off

If the Wireless LED stays off, check to see if the WiFi On/Off button on the router has been pressed. This button turns the wireless radio in the router on and off. The Wireless LED is lit when the wireless radio is turned on.

The WPS (Push 'N' Connect) Button Blinks Amber

If, after you use the WPS function, the WPS LED blinks green rapidly, check the following:

- Make sure that you have used the WPS button on the front of the router and not the WPS Wizard on the Add WPS Client screen.
- Check that PIN verification has succeeded for the wireless device you are adding to the wireless network.
- Make sure that you have not pressed the WPS button on the front of the router after disabling the WPS feature (you logged in to the router and disabled this previously).
- The router is stuck in the AP setup locked state (if you are using the wireless repeater function). To resolve this situation, either restart the router, or do the following:

  1. Select **Advanced > Advanced Setup > Wireless Settings**.

     The Advanced Wireless Settings screen displays.

  2. Select the **Enable Router's PIN** check box.
  3. Click the **Apply** button.

Cannot Log In to the Router

If you are unable to log in to the router from a computer on your local network, check the following:

- If you are using an Ethernet-connected computer, check the Ethernet connection between the computer and the router as described in the previous section.
- Make sure that your computer's IP address is on the same subnet as the router. If you are using the recommended addressing scheme, your computer's address should be in the range of 192.168.1.2 to 192.168.1.254.
- If your computer's IP address is shown as 169.254.x.x, recent versions of Windows and Mac OS generate and assign an IP address if the computer cannot reach a DHCP server. These autogenerated addresses are in the range of 169.254.x.x. If your IP address is in this range, check the connection from the computer to the router, and reboot your computer.
- If your router's IP address was changed and you do not know the current IP address, clear the router's configuration to factory defaults. This sets the router's IP address to 192.168.1.1. This procedure is explained in *Factory Settings* on page 133.
- Make sure that your browser has Java, JavaScript, or ActiveX enabled. If you are using Internet Explorer, click the **Refresh** button to be sure that the Java applet is loaded.
- Try quitting the browser and launching it again.
- Make sure that you are using the correct login information. The factory default login name is admin, and the password is password. Make sure that Caps Lock is off when you enter this information.
- If you are attempting to set up your NETGEAR router as an additional router behind an existing router in your network, either configure the NETGEAR router to function as an access point only (see *Wireless Access Point (AP)* on page 80) or consider replacing the existing router with the NETGEAR router.
- If you are attempting to set up your NETGEAR router as a replacement for an ADSL gateway in your network, the router cannot perform many gateway services, for example, converting ADSL or cable data into Ethernet networking information. NETGEAR does not support such a configuration.

Cannot Access the Internet

If you can access your router but you are unable to access the Internet, first determine whether the router can obtain an IP address from your Internet service provider (ISP). Unless your ISP provides a fixed IP address, your router requests an IP address from the ISP. You can determine whether the request was successful using the Router Status screen.

➢ **To check the WAN IP address:**

1. Start your browser, and select an external site such as *http://www.netgear.com*.
2. Access the router user interface at *http://www.routerlogin.net*.

3. Select the **Advanced** tab.

   The Router Status screen displays.

4. In the Internet Port pane, check that an IP address is shown for the Internet port.

   If 0.0.0.0 is shown, your router has not obtained an IP address from your ISP.

   For more information about the Internet Port pane, see *Internet Port Pane* on page 117.

If your router cannot obtain an IP address from the ISP, you might need to force your cable or DSL broadband modem to recognize your new router by restarting your network. For more information, see *Sequence to Restart Your Network* on page 123.

If your router is still unable to obtain an IP address from the ISP, the problem might be one of the following:

- Your Internet service provider (ISP) might require a login program.
  Ask your ISP whether they require PPP over Ethernet (PPPoE) or some other type of login.
- If your ISP requires a login, the login name and password might be set incorrectly.
- Your ISP might check for your computer's host name.
  Assign the computer host name of your ISP account as the account name in the Internet Setup screen.
- Your ISP allows only one Ethernet MAC address to connect to Internet and might check for your computer's MAC address. In this case, do one of the following:
  - Inform your ISP that you have bought a new network device, and ask them to use the router's MAC address.
  - Configure your router to clone your computer's MAC address.

Troubleshoot Internet Browsing

If your router can obtain an IP address, but your computer is unable to load any web pages from the Internet:

- Your computer might not recognize any DNS server addresses.

  A DNS server is a host on the Internet that translates Internet names (such as www addresses) to numeric IP addresses. Typically, your ISP provides the addresses of one or two DNS servers for your use. If you entered a DNS address during the router's configuration, reboot your computer, and verify the DNS address. You can configure your computer manually with DNS addresses, as explained in your operating system documentation.

- Your computer might not have the router configured as its TCP/IP gateway.

  If your computer obtains its information from the router by DHCP, reboot the computer, and verify the gateway address.

- You might be running login software that is no longer needed.

If your ISP provided a program to log you in to the Internet (such as WinPoET), you no longer need to run that software after installing your router. If you use Internet Explorer as your browser, you might need to select **Tools > Internet Options**, click the **Connections** tab, and select **Never dial a connection**. Other browsers have similar options.

Troubleshoot a PPPoE Internet Connection

➢ **To troubleshoot a PPPoE Internet connection:**

1. Start your browser, and select an external site such as *http://www.netgear.com*.
2. Access the router user interface at *http://www.routerlogin.net*.
3. Select the **Advanced** tab.

   The Router Status screen displays.
4. On the Internet Port pane, click the **Connection Status** button.

   For more information, see *Connection Status* on page 119. If the fields show valid information, including valid IP addresses, your PPPoE connection is up and working.

   If any of the fields show incomplete information, or no valid IP address, you can attempt to reconnect by clicking the **Connect** button. The router continues to attempt to connect indefinitely.

If you cannot connect after several minutes, you might be using an incorrect service name, user name, or password. There might also be a provisioning problem with your ISP.

Note: Unless you connect manually, the router does not authenticate using PPPoE until data is transmitted to the network.

Changes Not Saved

If the router does not save the changes you make through the NETGEAR genie screens, check the following:

- When you enter configuration settings on a screen, always click the **Apply** button before you move to another screen or tab, or your changes are lost.
- Click the **Refresh** or **Reload** button in the web browser. The changes might have occurred, but the old settings might be in the web browser's cache.

Wireless Connectivity

If you are having trouble connecting wirelessly to the router, try to isolate the problem.

- Does the wireless device or computer that you are using find your wireless network?

  If not, check the Wireless LED on the front of the router. It should be lit. If it is not, you can press the **Wireless** button on the side of the router to turn the router's wireless radio back on.

  If you disabled the router's SSID broadcast, your wireless network is hidden and does not show up in your wireless client's scanning list. (By default, SSID broadcast is enabled.)

- Does your wireless device support the security that you are using for your wireless network (WEP, WPA, or WPA2).
- If you want to view the wireless settings, select **Basic > Wireless Settings**. For more information, see *Basic Wireless Settings* on page 26.

Wireless Signal Strength

If your wireless device finds your network, but the signal strength is weak, check these conditions:

- Is your router too far from your computer, or too close? Place your computer near the router, but at least 6 feet away, and see whether the signal strength improves.
- Is your wireless signal blocked by objects between the router and your computer?

Troubleshoot Your Network Using the Ping Utility

Most network devices and routers contain a ping utility that sends an echo request packet to the designated device. The device then responds with an echo reply. You can easily troubleshoot a network by using the ping utility in your computer or workstation.

Test the LAN Path to Your Router

You can ping the router from your computer to verify that the LAN path to your router is set up correctly.

➢ **To ping the router from a computer running Windows:**

1. From the Windows toolbar, click the **Start** button, and then select **Run**.
2. In the field provided, type **ping** followed by the IP address of the router, as in this example:

   ping www.routerlogin.net

3. Click **OK**.

   You should see a message like this one:

   ```
   Pinging <IP address > with 32 bytes of data
   ```

   If the path is working, you see this message:

   ```
   Reply from < IP address >: bytes=32 time=NN ms TTL=xxx
   ```

   If the path is not working, you see this message:

   ```
   Request timed out
   ```

If the path is not functioning correctly, you could have one of the following problems:

- Wrong physical connections

  For a wired connection, make sure that the numbered LAN port LED is lit for the port to which you are connected.

  Check that the appropriate LEDs are on for your network devices. If your router and computer are connected to a separate Ethernet switch, make sure that the link LEDs are lit for the switch ports that are connected to your computer and router.

- Wrong network configuration

  Verify that the Ethernet card driver software and TCP/IP software are both installed and configured on your computer.

  Verify that the IP address for your router and your computer are correct and that the addresses are on the same subnet.

Test the Path from Your Computer to a Remote Device

After verifying that the LAN path works correctly, test the path from your computer to a remote device.

1. From the Windows toolbar, click the **Start** button, and then select **Run**.
2. In the Windows Run window, type:

   ping -n 10 <*IP address*>

   where <IP address> is the IP address of a remote device such as your ISP's DNS server.

If the path is functioning correctly, replies like those shown in the previous section are displayed.

If you do not receive replies:

- Check that your computer has the IP address of your router listed as the default gateway. If the IP configuration of your computer is assigned by a DHCP server, this information is not visible on your computer's Network Control Panel. Verify that the IP address of the router is listed as the default gateway.
- Check to see that the network address of your computer (the portion of the IP address specified by the subnet mask) is different from the network address of the remote device.

- Check that your cable or DSL broadband modem is connected and functioning.
- If your ISP assigned a host name to your computer, enter that host name as the account name in the Internet Settings screen.
- Your ISP could be rejecting the Ethernet MAC addresses of all but one of your computers.

Many broadband ISPs restrict access by allowing traffic only from the MAC address of your broadband modem, but some ISPs additionally restrict access to the MAC address of a single computer connected to that modem. If this is the case, configure your router to clone or spoof the MAC address from the authorized computer.

Supplemental Information

A

This appendix provides factory default settings and technical specifications for the N300 Wireless Router WNR2000v4:

- *Factory Settings*
- *Technical Specifications*

Factory Settings

You can return the router to its factory settings. Use the end of a paper clip or some other similar object to press and hold the **Restore Factory Settings** button on the back panel of the router for at least 7 seconds. The router resets, and returns to the factory settings. Your device returns to the factory configuration settings that are shown in the following table.

Table 4. WNR2000v4 router factory default settings

Feature		Default behavior
Router login	User login URL	www.routerlogin.com or www.routerlogin.net
	User name (case-sensitive)	admin
	Login password (case-sensitive)	password
Internet connection	WAN MAC address	Use default hardware address
	WAN MTU size	1500
	Port speed	Autosensing
Local area network (LAN)	LAN IP	192.168.1.1
	Subnet mask	255.255.255.0
	DHCP server	Enabled
	DHCP range	192.168.1.2 to 192.168.1.254
	Time zone	United States is Pacific time; otherwise, varies by region
	Time zone daylight saving time	Disabled
Wireless	Wireless communication	Enabled
	SSID name	Preset. For information, see the router label. (For a description of the router label, see *Label* on page 11.)
	Network key (password)	
	Broadcast SSID	Enabled
	Transmission speed	Auto **Note:** The maximum wireless signal rate derived from IEEE Standard 802.11 specifications. Actual throughput varies. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, lower actual data throughput rate.
	Country/region	United States in the US; otherwise varies by region
	RF channel	Auto
	Operating mode	Up to 150 Mbps

Table 4. WNR2000v4 router factory default settings (continued)

Feature		Default behavior
Wireless (continued)	20/40 MHz coexistence	Enabled
	Data rate	Best
	Output power	Full

Technical Specifications

Table 5. WNR2000v4 router specifications

Feature	Description
Data and routing protocols	TCP/IP, RIP-1, RIP-2, DHCP, PPPoE, PPTP, Bigpond, Dynamic DNS, UPnP, and SMB
Power adapter	• North America: 120V, 60 Hz, input • UK, Australia: 240V, 50 Hz, input • Europe: 230V, 50 Hz, input • All regions (output): 12V DC @ 1A, output
Dimensions	178 x 130 x 54 mm (7 x 5.1 x 2.1 in.)
Weight	0.28 kg (0.62 lb)
Operating temperature	0° to 40°C (32º to 104ºF)
Operating humidity	90% maximum relative humidity, noncondensing
Electromagnetic Emissions	FCC Part 15 Class B VCCI Class B EN 55 022 (CISPR 22), Class B C-Tick N10947
LAN	10BASE-T or 100BASE-Tx, RJ-45
WAN	10BASE-T or 100BASE-Tx, RJ-45
Wireless	Maximum wireless signal rate complies with the IEEE 802.11 standard. See the footnote for the previous table.
Radio data rates	Auto Rate Sensing
Data encoding standards	IEEE 802.11n version 2.0 IEEE 802.11n, IEEE 802.11g, IEEE 802.11b 2.4 GHz
Maximum computers per wireless network	Limited by the amount of wireless network traffic generated by each node (typically 50–70 nodes).
Operating frequency range	2.412–2.462 GHz (US) 2.412–2.472 GHz (Japan) 2.412–2.472 GHz (Europe ETSI)
802.11 security	WEP, WPA-PSK, WPA2-PSK, WPA-PSK + WPA2-PSK mixed mode, WPA/WPA2 Enterprise

Notification of Compliance

B

NETGEAR Wireless Routers, Gateways, APs

Regulatory Compliance Information

This section includes user requirements for operating this product in accordance with National laws for usage of radio spectrum and operation of radio devices. Failure of the end-user to comply with the applicable requirements may result in unlawful operation and adverse action against the end-user by the applicable National regulatory authority.

This product's firmware limits operation to only the channels allowed in a particular Region or Country. Therefore, all options described in this user's guide may not be available in your version of the product.

Europe – EU Declaration of Conformity

Products bearing the CE marking comply with the following EU directives:

- EMC Directive 2004/108/EC
- Low Voltage Directive 2006/95/EC

If this product has telecommunications functionality, it also complies with the requirements of the following EU Directive:

- R&TTE Directive 1999/5/EC

Compliance with these directives implies conformity to harmonized European standards that are noted in the EU Declaration of Conformity.

Intended for indoor use only in all EU member states, EFTA states, and Switzerland.

This device may not be used for setting up outdoor radio links in France and in some areas the RF output power may be limited to 10 mW EIRP in the frequency range of 2454 - 2483.5 MHz. For detailed information the end-user should contact the national spectrum authority in France.

FCC Requirements for Operation in the United States

FCC Information to User

This product does not contain any user serviceable components and is to be used with approved antennas only. Any product changes or modifications will invalidate all applicable regulatory certifications and approvals.

FCC Guidelines for Human Exposure

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance of 20 cm between the radiator and your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

FCC Declaration of Conformity

We, NETGEAR, Inc., 350 East Plumeria Drive, San Jose, CA 95134, declare under our sole responsibility that the N300 Wireless Router WNR2000v4 complies with Part 15 Subpart B of FCC CFR47 Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference, and
- This device must accept any interference received, including interference that may cause undesired operation.

FCC Radio Frequency Interference Warnings & Instructions

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following methods:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment into an electrical outlet on a circuit different from that which the radio receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution

- Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.
- This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.
- For product available in the USA market, only channel 1~11 can be operated. Selection of other channels is not possible.
- This device and its antenna(s) must not be co-located or operation in conjunction with any other antenna or transmitter.

TV Tuner (on Selected Models)

Note to CATV System Installer: This reminder is provided to call the CATV system installer's attention to Section 820-93 of the National Electrical Code, which provides guidelines for proper grounding and, in particular, specifies that the Coaxial cable shield be connected to the grounding system of the building as close to the point of cable entry as possible.

Canadian Department of Communications Radio Interference Regulations

This digital apparatus (N300 Wireless Router WNR2000v4) does not exceed the Class B limits for radio-noise emissions from digital apparatus as set out in the Radio Interference Regulations of the Canadian Department of Communications.

This Class [B] digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe [B] est conforme à la norme NMB-003 du Canada

Industry Canada

This device complies with RSS-210 of the Industry Canada Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Ce dispositif est conforme à la norme CNR-210 d'Industrie Canada applicable aux appareils radio exempts de licence. Son fonctionnement est sujet aux deux conditions suivantes: (1) le dispositif ne doit pas produire de brouillage préjudiciable, et (2) ce dispositif doit accepter tout brouillage reçu, y compris un brouillage susceptible de provoquer un fonctionnement indésirable.

IMPORTANT NOTE: Radiation Exposure Statement:

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

NOTE IMPORTANTE: Déclaration d'exposition aux radiations:

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 20 cm de distance entre la source de rayonnement et votre corps.

Interference Reduction Table

The table below shows the Recommended Minimum Distance between NETGEAR equipment and household appliances to reduce interference (in feet and meters).

Household Appliance	Recommended Minimum Distance (in feet and meters)
Microwave ovens	30 feet / 9 meters
Baby Monitor - Analog	20 feet / 6 meters
Baby Monitor - Digital	40 feet / 12 meters
Cordless phone - Analog	20 feet / 6 meters
Cordless phone - Digital	30 feet / 9 meters
Bluetooth devices	20 feet / 6 meters
ZigBee	20 feet / 6 meters

Index

Numerics

20/40 MHz coexistence, disabling 75
6to4 tunnel, IPv6 Internet connection 107

A

access list, wireless clients 78
access point (AP) mode 80
accessing
    remote computer 86
    router remotely 100
active static route 99
address reservation 49
advertisement period, UPnP 102
AES (Advanced Encryption Standard) 29
alerts, emailing 66
ALG (Application Layer Gateway) 44
applications, QoS for 54
attached devices, viewing 32
authentication, required by mail server 67
autoconfiguration, IPv6 Internet connection 105
autodetection, IPv6 Internet connection 104

B

back panel 10
backing up configuration 71
bandwidth control, QoS 58
bandwidth, inbound and outbound 118
base station, wireless distribution system 83
blocking
    inbound traffic 86
    keywords and sites 61
    services 63
    wireless clients 78
box contents 8
browsing, troubleshooting 127

C

cables, checking 123
changes not saved, router 128
channel, wireless 28
coexistence 20/40 MHz, disabling 75
compliance 135
configuration file, managing 71
connecting wirelessly, operating range 11
connection status 119
contents, box 8
crossover cable 125
CTS/RTS threshold 76
custom service, port forwarding 91

D

dashboard, described 19
data packets, fragmented 45
DDNS (Dynamic DNS) 96
default DMZ server 44
default factory settings
    list of 133
    restoring 72
default gateway 119
deleting configuration 72
denial of service (DoS)
    attacks 43, 71
    protection 60
devices attached, viewing 32
DHCP (Dynamic Host Configuration Protocol) server
    IPv6 Internet connection 110
    managing router's 48
    viewing 119
dimensions, router 134
DMZ server 44
DNS (Domain Name Server) addresses
    Internet connection, configuring 26
    troubleshooting 127
    viewing 118–119
domain name 25
domains, blocking 61
DoS (denial of service)
    attacks 43, 71
    protection 60
Dynamic DNS (DDNS) 96

Dynamic Host Configuration Protocol (DHCP) server
IPv6 Internet connection 110
managing router's 48
viewing 119
DynDNS.org 96

E

electromagnetic emissions 134
email notices 66
erasing configuration 72
Ethernet cables, checking 123
Ethernet LAN port LEDs
described 9
troubleshooting 125

F

factory default settings
list of 133
restoring 72
filtering IPv6 packets 105
firmware
upgrading 18, 69
version 117
fixed IPv6 address, IPv6 Internet connection 108
fragmentation length 76
fragmented data packets 45
front panel 9

G

games, DMZ server 44
gateway
default 119
IP address 26
genie, NETGEAR 17
guest network
setting up 36
viewing 121
GUI, described 19

H

hardware, version 117
hops, UPnP 102
host name 25
host, trusted 62
humidity, operating 134

I

IGMP proxy 44
inbound bandwidth 118
inbound traffic, allowing or blocking 86
interference 75
Internet connection
setting up 24
status 119
troubleshooting 17, 126
Internet LED
described 9
troubleshooting 125
Internet port
manually setting up 24
Setup Wizard, using to connect 17, 41
viewing setting 117
Internet Relay Chat (IRC) 87
Internet service provider (ISP)
account information 16
setting up a connection 25
Internet services, blocking access 63
IP addresses
Dynamic DNS (DDNS) 96
reserved 49
setting up 25–26
viewing 117–120
IPv6 Internet connection 103
IRC (Internet Relay Chat) 87
isolation, wireless 28, 36

K

keywords, blocking 61

L

L2TP 25
label, product 11
LAN port
QoS for 55
viewing settings 117
LAN port LEDs
described 9
troubleshooting 125
LAN, setting up 46
lease, DHCP 119
LEDs
descriptions 9
troubleshooting, using for 124–125
verifying cabling 14
Live Parental Controls 33
local servers, port forwarding to 90
logging in
router 18
troubleshooting 126

types of 16
logs
emailing 66
setting up 71
viewing 70

M

MAC addresses
product label 11
QoS for 56
router's 26
mail server, outgoing 66
managing router remotely 100
maximum transmit unit (MTU) size 45
menus, described 19
metering traffic 112
metric values, static routes 99
mixed mode wireless security option 29
mode
router operation 117
wireless 28
MTU (maximum transmit unit) size 45
multicasting 48

N

NAT (Network Address Translation) 44
NETGEAR genie 17
network settings, troubleshooting 123
network, guest
setting up 36
viewing 121
newsgroups 61

O

online games
DMZ server, using 44
QoS for 54
open NAT 44
operating frequency range 134
operating mode, router 117
outbound bandwidth 118
outgoing mail server 66

P

packets
fragmented 45
transmitted and received 118
parental controls 33
passphrases
changing 29
product label 11
pass-through, IPv6 Internet connection 108
password recovery, administrative 21
password, default 18
permanent IP address 26
PIN method, WPS 42
PIN, viewing and configuring 77
ping, responding 43
plug and play 101
Point-to-Point Tunneling Protocol (PPTP)
Internet connection 25
viewing connection status 120
policies, QoS 52
port filtering 63
port forwarding
concepts 86
configuring 90
port numbers, services 63
port triggering 87
concepts 86
configuring 93
portmap table, UPnP 102
ports
back panel 10
status, viewing 118
positioning the router 11
power adapter, specifications 134
Power LED
described 9
troubleshooting 124
PPPoE (PPP over Ethernet) 127
IPv4 Internet connection 25
IPv6 Internet connection 111
troubleshooting 128
viewing connection status 120
PPTP (Point-to-Point Tunneling Protocol)
Internet connection 25
viewing connection status 120
preamble mode 76
preset security
described 26
passphrase 29
primary DNS address 26
prioritizing traffic 51–57
private static route 99
protection, Internet 33
Push 'N' Connect 22
push button method, WPS 41

Q

QoS (Quality of Service) 51–59

R

radio, disabling 75
RADIUS server 30
range of wireless connections 11
received packets 118
recovering administrative password 21
releasing and renewing connection status 120
remote management 100
repeater, wireless distribution system 84
reserved IP adresses 49
restarting network 123
restoring
  configuration file 72
  default factory settings 72, 133
RIP (Router Information Protocol)
  setting up 47
  static routes 99
router interface, described 19
router status, viewing 116
routes, static 98
rules, QoS 52

S

saving changes, troubleshooting 128
scheduling
  keyword and service blocking 65
  wireless service 76
secondary DNS addresses 26
secured NAT 44
security
  firewall settings 60–67
  wireless settings 26–32
security PIN, WPS 42
sending logs by email 66
serial number, product label 11
services
  blocking 63
  port forwarding 91
  port triggering 95
Session Initiation Protocol Application Layer Gateway (SIP ALG) 44
settings, default
  list of 133
  restoring 72
Setup Wizard 40
shared key, WEP 31
signal strength, troubleshooting 129
SIP ALG (Session Initiation Protocol Application Layer Gateway) 44
sites, blocking 61
SMTP server 66
software
  upgrading 18, 69
  version 117
specifications, technical 134
SSID
  described 28
  product label 11
stateful packet inspection (SPI) firewall 105
static IP addresses
  IPv4 Internet connection 26
  IPv6 Internet connection 108
static routes 98
statistics, traffic 118
status, viewing (router, Internet, and networks) 116–121
system up time 118

T

technical specifications 134
technical support 2
temperatures, operating 134
Temporal Key Integrity Protocol (TKIP) 29
time to live, advertisement, UPnP 102
time-out, port triggering 94
tips, troubleshooting 123
TKIP (Temporal Key Integrity Protocol) 29
trademarks 2
traffic
  metering 112
  prioritizing 51–57
  statistics, viewing 118
transmitted packets 118
troubleshooting 122–131
trusted host 62

U

Universal Plug and Play (UPnP) 101
up time, system 118
upgrading firmware 18, 69
uplink bandwidth 58
user interface, described 19
user name, default 18

V

versions, firmware, hardware, and language 117
videoconferencing, DMZ server 44
viewing
  logs 70
  router, Internet, and network status 116–121
VoIP (Voice over IP) 44

W

WAN IP address, troubleshooting 126
WAN port
  manually setting up 24
  Setup Wizard, using to connect 17, 41
  viewing settings 117
WAN port LED
  described 9
  troubleshooting 125
web server, port forwarding 92
weight, router 134
WEP (Wired Equivalent Privacy) 31
Wi-Fi Multimedia (WMM) 51
Wi-Fi Protected Setup (WPS) 22, 41
Wired Equivalent Privacy (WEP) 31
wireless channel 28
wireless clients, restricting access 78
wireless connections
  operating range 11
  troubleshooting 129
wireless devices, adding to network 21
wireless distribution system (WDS) 82
wireless isolation 28, 36
Wireless LED
  described 9
  troubleshooting 125
wireless mode 28
wireless network name (SSID)
  broadcasting 28
  described 28
  product label 11
wireless network settings 28
wireless radio, disabling 75
wireless repeating 82
wireless security options 28–32
wireless settings
  described 28
  troubleshooting 123
  viewing 120
wireless signal strength, troubleshooting 129
wireless signal, turning off 76
wizards
  Setup Wizard 40
  WPS Wizard 41
WMM (Wi-Fi Multimedia) 51
WPA/WPA2 Enterprise 30
WPA-PSK, WPA2-PSK, and WPA+WPA2 mixed mode 29
WPS button 22
WPS LED
  described 10
  troubleshooting 125
WPS settings 77
WPS Wizard 41